

St Petersburg State University  
Graduate School of Management

Master in Management Program

FRAMEWORK DEVELOPMENT OF SECURITY SYSTEM ASSESSMENT  
FOR RETAIL OUTLETS

Master's Thesis by the 2<sup>nd</sup> year student  
Marina Syromyatnikova

Concentration – Information Technologies &  
Innovations Management

Research advisor:  
Nikolay A. Zenkevich, Associate Professor

St Petersburg

2017

**ЗАЯВЛЕНИЕ О САМОСТОЯТЕЛЬНОМ ХАРАКТЕРЕ ВЫПОЛНЕНИЯ  
ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**

Я, Сыромятникова Марина Алексеевна, студент второго курса магистратуры направления «Менеджмент», заявляю, что в моей ВКР на тему  
«Разработка методик оценки систем безопасности розничной торговли»  
.....»,  
представленной в службу обеспечения программ магистратуры для последующей передачи в государственную аттестационную комиссию для публичной защиты, не содержится элементов плагиата.

Все прямые заимствования из печатных и электронных источников, а также из защищенных ранее выпускных квалификационных работ, кандидатских и докторских диссертаций имеют соответствующие ссылки.

Мне известно содержание п. 9.7.1 Правил обучения по основным образовательным программам высшего и среднего профессионального образования в СПбГУ о том, что «ВКР выполняется индивидуально каждым студентом под руководством назначенного ему научного руководителя», и п. 51 Устава федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет» о том, что «студент подлежит отчислению из Санкт-Петербургского университета за представление курсовой или выпускной квалификационной работы, выполненной другим лицом (лицами)».

С.С. (Подпись студента)

26/05/2017 (Дата)

**STATEMENT ABOUT THE INDEPENDENT CHARACTER  
OF THE MASTER THESIS**

I, Marina Syromyatnikova, (second) year master student, \_\_\_\_\_ program  
«Management», state that my master thesis on the topic  
«Framework development of security system assessment for retail outlets»  
.....»,

which is presented to the Master Office to be submitted to the Official Defense Committee for the public defense, does not contain any elements of plagiarism.

All direct borrowings from printed and electronic sources, as well as from master theses, PhD and doctorate theses which were defended earlier, have appropriate references.

I am aware that according to paragraph 9.7.1. of Guidelines for instruction in major curriculum programs of higher and secondary professional education at St. Petersburg University «A master thesis must be completed by each of the degree candidates individually under the supervision of his or her advisor», and according to paragraph 51 of Charter of the Federal State Institution of Higher Professional Education Saint-Petersburg State University «a student can be expelled from St. Petersburg University for submitting of the course or graduation qualification work developed by other person (persons)».

С.С. (Student's signature)

26/05/2017 (Date)

## АННОТАЦИЯ

Автор	Марина Сыромятникова
Название магистерской диссертации	Разработка методики оценки системы безопасности объектов розничной торговли.
Факультет	Высшая Школа Менеджмента
Направление подготовки	Менеджмент
Год	2017
Научный руководитель	Николай Анатольевич Зенкевич, к. ф-м. н., доцент кафедры операционного менеджмента ВШМ
Описание цели, задач и основных результатов	<p><b>Основная цель:</b> Разработать методику оценки системы безопасности для объектов розничной торговли, позволяющую определить слабые элементы системы безопасности и разработать специфические рекомендации по ее улучшению.</p> <p><b>Основные задачи:</b></p> <ul style="list-style-type: none"> <li>• Установить критерии оценки системы безопасности на основе исследования научной литературы и анализа практического опыта</li> <li>• Разработать методику оценки системы безопасности для объектов розничной торговли на основе выбранных критериев и количественной оценки результатов анкетирования</li> <li>• Применить методику на выбранных кейс-компаниях, чтобы проиллюстрировать что она позволяет определить слабые элементы системы безопасности и разработать специфические рекомендации по ее улучшению</li> </ul> <p><b>Основные результаты:</b></p> <ul style="list-style-type: none"> <li>• Установлены критерии оценки системы безопасности и представлены в форме иерархической системы показателей</li> <li>• АПИС был определен как наиболее подходящий метод количественной оценки результатов анкетирования</li> <li>• Разработана методика оценки системы безопасности для объектов розничной торговли</li> <li>• Методика была применена на кейс-компаниях, что позволило определить слабые элементы систем безопасности и пути их улучшения</li> </ul>
Ключевые слова	Разработка методики, система безопасности, АПИС, ритейл, безопасность в розничной торговле

## ABSTRACT

Master student's name	Marina Syromyatnikova
Master Thesis Title	Framework development of security system assessment for retail outlets.
Faculty	Graduate School of Management
Main field of study	Master in Management
Year	2017
Academic advisor's name	Nikolay A. Zenkevich, Associate Professor, Department of Operations Management, GSOM
Description of the goal, tasks and main results	<p><b>Main goal:</b> To develop a framework of security system assessment for retail outlets, allowing to identify the weak elements of security system and to develop specific recommendations on its improvement.</p> <p><b>Research tasks:</b></p> <ul style="list-style-type: none"> <li>• Determine criteria of security system assessment on the basis of scientific literature research and practical experience analysis</li> <li>• Develop a framework of security system assessment for retail outlets on the basis of selected criteria and quantitative evaluation of the questionnaire results</li> <li>• Apply the framework on the selected case companies to illustrate that it allows to identify the weak elements of security system and to develop specific recommendations on its improvement</li> </ul> <p><b>Main results:</b></p> <ul style="list-style-type: none"> <li>• Criteria of security assessment were identified and presented in the form of hierarchic system of indicators</li> <li>• APIS was identified to be the most suitable method of quantitative evaluation of questionnaire results</li> <li>• The framework of security system assessment for retail outlets was developed</li> <li>• The framework was applied on the case companies which allowed to identify weak elements of security systems and ways to improve it</li> </ul>
Keywords	Framework development, security system, APIS, retail outlets, security in retail industry

## TABLE OF CONTENT

INTRODUCTION .....	6
CHAPTER 1. SECURITY IN RETAIL INDUSTRY .....	8
1.1. Defining security in context .....	8
1.2. Business entities' security system fundamentals .....	15
1.3. Retail outlets' security system specifics .....	27
1.4. Hierarchic system of criteria of security system assessment.....	33
CHAPTER 2. SECURITY SYSTEM ASSESSMENT FOR RETAIL OUTLETS .....	37
2.1. Research methodology.....	37
2.2. Methods for multi criteria selection of alternatives .....	38
2.3. Framework of security system assessment.....	49
CHAPTER 3. APPLICATION OF THE FRAMEWORK TO THE CASE OUTLETS .....	53
3.1. Retail business and case companies description.....	53
3.2. Framework application .....	56
RESULTS AND DISCUSSION .....	66
CONCLUSION .....	71
REFERENCES .....	73
APPENDICES .....	78
Appendix 1. Questionnaire results: relative importance of characteristics .....	78
Appendix 2. Questionnaire: relative importance of characteristics .....	81
Appendix 3. Additional Output from APIS .....	85

## INTRODUCTION

As the topic suggests, the following work will present a framework of security system assessment for retail outlets. The main focus of this work is the issue of security in retail industry. This topic was chosen because the preliminary research showed that the topic is current and important, and later this assumption was confirmed by both scholars and practitioners. Multiple researchers, including Knezevic et al (2016) and Koh et al (2003) have talked about retail industry and stated in their articles that security, theft, and losses are among the major issues in retail industry. Moreover, the practitioners that were interviewed, mainly representatives of companies that engineer, install and sell security systems, have confirmed the fact that security is a major issue in retail. Indeed, according to the opinion of the interviewees, retailers regularly face losses and are striving to minimize them. This is especially true in the context of slow economic growth and recent economic crisis in Russia. If before the retailers were able to realize larger losses, currently the majority of retailers find cutting losses as a valuable way to save money in the environment of slow economic growth. The current economic conditions make the issue of security more prominent for retailers than ever.

The preliminary research also has revealed that although the advantages and disadvantages of security systems are extensively covered in the literature, how to approach the improvement of security in a given retail store is not that clear. There is no widely accepted comprehensive methodology or framework on how to act when the management is willing to minimize losses through security level improvement. The author assumes that in order to minimize losses and improve the overall security level of the store, the management first has to conduct a thorough assessment of the current state, because oftentimes some elements of security system, such as required fire alarm system, are already installed and it is important to assess the condition of currently installed elements. In the situation when the store has been operating already and is not a newly opened store, the key is, as the author of this work assumes, in the proper assessment of the security system that is currently exists in the store. Knowing the advantages and the disadvantages of the security system, as the author of this work assumes, will give the basis for development of the strategies for improvement and will be the first step towards losses minimization.

A proper security system assessment framework, therefore, is considered to be a mean of combatting the issue of losses, a mean of increasing the level of security, and a mean of prevention of theft, fraud and errors. The framework is assumed to make better security possible by bridging the gap between the knowledge about security systems and knowledge about the origin of losses in retail industry.

The main goal of this work is to develop a framework of security system assessment for retail outlets, allowing to identify the weak elements of security system and to formulate specific recommendations on its improvement.

The current work is organized in three chapters; a corresponding objective is allocated for each chapter. The objectives of the work are:

- To determine criteria for security system assessment on the basis of scientific literature research and practical experience analysis
- To develop a framework of security system analysis for retail outlets on the basis of selected criteria and quantitative evaluation of the questionnaire results
- To apply the framework on the selected case companies in order to illustrate that the framework allows to identify the weak elements of security system and to develop recommendations on its improvement

The major structure elements of the thesis are introduction, three chapters, results and discussion, conclusion, references and appendices. Accordingly, the in the first chapter the author is aiming to determine key elements of security system assessment process on the basis of both scientific literature research and practical experience analysis. In the second chapter, the aim is to identify the most suitable method for analysis of these elements through research and comparison of applicable methods and on its basis develop a framework of security system assessment for retail outlets. In the third chapter, the aim is to apply the framework on the selected case companies in order illustrate that the framework allows to identify the weak elements of security system and to develop recommendations on its improvement. The numbering of the tables and figures consists of two digits, first corresponding to the number of the chapter and second corresponding to the number of the table or figure for easy navigation throughout the pages. Each chapter begins with a short introduction and ends with the concluding paragraph. The summary and main results are presented in “results and discussion” section.

The following work shows a way for a complete application of the framework from the scratch to recommendations, which can be repeated either in full of starting after the elements identification if it is applied in the context of retail industry. The developed framework is a flexible tool and the application of the framework allows managers to identify the weak elements in the existing security system and to develop specific recommendations on its improvement. The effect of the execution of recommendations will be the minimization of losses, which is a current and important problem that retailers face of a regular basis.

## CHAPTER 1. SECURITY IN RETAIL INDUSTRY

The aim of the first chapter is to determine criteria for security system assessment process on the basis of scientific literature research and practical experience analysis. In section 1.1 the various definitions of the term “security” as well as the terms closely related to the concept of security are examined, and the first section concludes with the collective definition of the term “security” that will be used throughout the following thesis. The section 1.2 discusses the security system fundamentals related to the security of business entities in general. This section concludes with the formulated basic concepts related to the security system assessment of a business entity. Section 1.3 is also focused on the security systems, only the range of business entities is narrowed down to retail outlets only and specific peculiarities of the retail outlets security system assessment are discussed. Section 1.3 ends with the list of criteria that was formulated through literature research. This list of criteria is further confirmed and expanded through the in-depth interviews and the final version of the list of criteria is presented in Section 1.4 in the form of the hierarchic system of criteria. Chapter 1 ends with the hierarchic system of criteria of security system assessment.

### 1.1. Defining security in context

The notion of security encompasses multiple aspects and is applicable in various contexts. Definitions of term «security» as part of a given discipline or field can have substantial differences. At the origin of the thesis it is deemed necessary to provide some definitions of the mentioned term and a range of interconnected concepts.

In accordance with Merriam-Webster dictionary (2017) security is defined as a state of being secure. This is one of the most commonly used meanings, which derives from Latin «*securitas*» going back to XV century. Subsequently the definition broadened by covering such meanings as «something that secures», «safety of the state, person etc. » and even «property in bonds». Stone (2007) defines the essence of security as the protection of people, information and property. The word «secure», which is key to the security definition, is specified as being free from danger or free from risk of loss. Such definitions link security with concepts of risk and threat. The term «security» can be applied to any valuable assets, which in business environment include cash, inventory, land and buildings, people, intellectual property and information etc.

Security professional C.E. Marcum (1979) in his works defines security as establishment and maintenance of specialized activities and procedures intended for protection of personnel, property and enterprise mission from destruction, disruption, impairment, or other loss due to deliberate and willful incidents of fraud, theft, pilferage, vandalism, sabotage, riot or mob action.



Analogous definition is provided by Business Dictionary: security is the prevention of and protection against assault, damage, fire, fraud, invasion of privacy, theft, unlawful entry, and other such occurrences caused by deliberate action. Within these definitions the range of possible threats is encircled. It is worthy to note that contemporary world formation and technological progress lead to occurrence of new emergent threats. Innovation technologies provide both opportunities and threats to the community. Slightly different point of view on the security concept is presented by Ura (2015). In compliance of his work security is «the degree of resistance or protection against harm». Contrary to preceding definitions, this one determines security not as a state or a process, but as a degree of protection.

To gain a better understanding of security concept several related terms should be analyzed, such as threat, crime, risk, security system, security functions and areas, security object. All these terms highlight different dimensions of security concept.

The term “threat” refers to an activity that may potentially be harmful to security. Threat is «an intention and capability of an adversary to undertake actions that would be harmful to a person, facility, or other valuable asset». Knowledge of potential threats allows decision maker to understand motivation behind potentially harmful behavior (Sylvie et al., 2013). The significance of damage that will happen if the threat is not mitigated is called impact. The list of threats is almost endless, and its content depends on the variety of situational factors. Analysis of security should be carried out in the light of the foregoing. Assessment of threats is the first phase of risk evaluation. The major impact that is considered in this thesis is economic losses. Therefore, only the threats that lead to economic losses will be considered in this thesis.

One of the most common threats to security is crime. According to the expert opinion, crime is a conduct in violation of the laws of the state or federal government, or local jurisdiction for which there is no legally acceptable justification (Schmalleger, 2013). The term «crime» is thought as any abusive practices and wrongful acts, which can harm the impacted object. From the security perspective the growth and expansion of criminal practices constitutes a prominent menace. Crime can be distinguished from other threats by its large variety of forms. From olden times to the time being the most common form of criminal action is theft. Nowadays theft can be committed not only of the tangible objects, but also of the intangible valuable assets, such as information or intellectual property. Recently emerged forms of theft and other criminal action lay under a necessity to develop new security methods.

The risk concept is also commonly used in security literature. Multidimensionality and complexity of risk phenomena conducted widening of this concept and emergence of a set of heterogeneous definitions. Risk can be mathematically defined as the probability of event occurrence multiplied by its impact. It is defined through likelihood and impact, while impact is

generally measured in monetary terms (Petruzzi et al., 2016). One of the clearest definitions of the risk is due to Lowrance (1976): «risk is a measure of a probability and severity of adverse effects». Consequently the riskiness of the object is explicitly interconnected with its security degree.

Another concept that has to be defined is security system. Oxford dictionary (2017) defines it as «any system that is put in place in order to maintain security of a person or thing». Referring to a widely accepted definition of a system, the system is a combination of elements and connections in between them. Similarly to this definition, security system can be defined as a combination of elements of the security system and connections in between these elements. Security systems typically have an aim to protect something. Security systems range from fairly simple systems, such as fire alarm system, to sophisticated security systems which are specifically engineered for a particular goal and a specified secured object. Usually security system corresponds to some safety kit, including methods and techniques of detecting, preventing and protecting from different threat types. Security system development includes series of steps and activities to be done:

- Predictive modeling, recognition, analysis and estimation of threats;
- Specification of key dimensions of security enforcement;
- Regulatory management in the field of security;
- Development and application of the comprehensive set of measures to define, prevent and dispose threats, localize and counteract threat manifestation;
- Appliance of economic measures for provision of security;
- Implementation and usage of focused technical findings and facilities in order to provide security;
- Organizing scientific activities and research in the sphere of security;
- Coordination of activities and procedures concerning maintenance of security;
- Financing accrued expenses for the purposes of security protection and budget management;
- Cooperation with people and firms, who deal with analogous threats, and joint operations performance in the area of security.

Uraic and Pagano in their academic paper concentrate on functional area of security management (Pagano, Uraic, 1974). According to their opinion, seven managerial functions are highlighted in the sphere of organizational security:

1. Planning for security – preparatory acts for process of security system implementation;
2. Organizing for security – establishment of security system;
3. Staffing for security – security staff recruitment and selection;
4. Directing organizational security – maintenance of security system operation;
5. Controlling organizational security - exploitation of action framework aimed on performance control and progress monitoring;
6. Representation for organized security – endowment stakeholders with information about security;
7. Innovating for organizational security – application of scientific and accomplishments for purposes of security enforcement.

Stated above functions are interdependent and their effective implementation is attributable to some supportive factors. Such factors are by nature of technologies and include information technology, identification technology, investigation technology, instrumentation technology and inspection technology (Pagano, Uraic, 1974). Totality of enumerated technologies allows building up effective security system, maximizing security performance and maintaining management functions in the area of organizational security.

In accordance with Knight and Richardson realization of security functions requires some categories of technical assistance (Knight, Richardson, 1963). These categories also include information, investigation, identification along with impediments, movement and traffic control, procedural controls, patrol activities, education and training, special techniques and equipment. All the categories should be expressed by instructions, reports, morale and efficiency factors, and inspections. Mentioned instruments and factors depict operational aspects of the security system.

Another expert in security sphere, San Luis, distinguished six functional areas of security: lines of defense, developing the security function, security survey, security operations, equipment for security and management's responsibility (San Luis, 1973). Notwithstanding the differences within the nomenclature of security functions, proposed by various specialists, the subject matter of them is identical.

From there, security system encompasses the full range of actions and ways of security enforcement. Security systems can be general-purpose or particularized. General-purpose security systems blanket maximum possible types of threats, whereas particularized systems are targeted at specific problem solution, for example, information security system or firefighting

system. Another example of security system is electronic system that alarms in case of intrusion, electronic article surveillance, CCTV, etc. (Firesmith, 2003).

Every security system regardless to its purpose and use can be decomposed into a number of components. Mandelbaum claims that protective system generally consists of the following elements (Mandelbaum, 1973):

- Physical barriers – perimeter, exterior and interior of the secured facility;
- Alarm and control electronic subsystems;
- Communication system and connection with external emergency agencies, such as police, rescue and firefighting services;
- Counterforces, such as guards or watchman;
- Center of control and communication;
- Administrative staff as representative of security management;
- Plan of standard security operations, schedules and allocation of responsibilities;
- Operational and emergency procedures.

Attention should be paid to each of these elements with the purpose to build an effective security system, which helps to avoid threats or even though minimize their impacts. Mandelbaum also suggests functional organizational structure for high-performance security system (Mandelbaum, 1973). Basic version of this structure includes five divisions – administrative, investigation, guard, firefighting and security management. Every division is in charge of implementation of some security function or range of functions.

In order for effective implementation of security functions except for organizational structuring some security subject should be taken into account. The list of these subjects was suggested by Wathen and includes pride in professionalism, rewarding human relations, patrols, guiding, protection aids, effective communication etc. (Wathen, 1972). From this list it may be concluded that human factor is especially critical in security enforcement process.

Woodruff asserts that irrespective of differences between the security systems of various companies three basic vectors can be emphasized – private protection, fire protection and personnel safety (Woodruff, 1974). These vectors address to main security industry sectors. Today's evolving technology landscape enables to fill up this list with information security. The character of security services market derives from the key functional areas of security, which, as provided by Uraic and Pagano (Pagano, Uraic, 1974), are physical security, personnel security and proprietary information security. Similar scope of security functions is presented in Knight and Richardson's paper about security (Knight, Richardson, 1963). They identify five security

areas: besides physical and personnel security, communication and technological security and emergency planning are included.

The list of security components was complemented by Kingsbury and Post (Kingsbury, Post, 1977) with planning process, organization for security and security training and education. That sort of attitude to functional areas of security reminds of the security system essence in terms of functional activities. The confluence of mentioned terms and concepts is confirmed by Healy and Walsh, who suggest seven interrelated security functions (Healy, Walsh, 1971). In accordance with their work security consists of physical security, emergency and disaster, fire protection, guards, investigations, security of documents and personnel security.

While studying the concept of security it is critical to pay attention to security object notion. Every organization regardless of its specifics and business activity has similar basic types of vulnerable assets. By vulnerable asset object liable to security threats is meant. Security threats can include theft, destruction, fraud, unauthorized disclosure etc. The vulnerable assets are subjects to similar types of security threats. These threats come from attackers and these similarities in types of threat and types of attack lead to considerable similarities when it comes to security mechanisms that are used to guard vulnerable assets from the threats imposed by attackers. Security requirements hence tend to be of similar nature in various industries (Firesmith, 2003). Another aspect of security concern is personnel security – the problem of great significance. Staff within the organization should on the one hand understand the importance of security measures and maintain existing security system and on the other hand feel sense of personal safety during the work process. At the same time established security system is instrumental in clearing employees of suspicion if, for example, theft occurs.

Secured objects can be of various types and hence are being classified into categories. Security instruments and actions depend on the nature of secured object. Secured object is an enterprise, store, bank, house, building, office, part of it or a combination that is equipped with the security system. In the business environment these secured objects are places where valuable assets and resources are stored. These valuable assets and resources help businesses maintain competitiveness in the market. Because of the value of such resources, they should be properly protected. Valuable and vulnerable assets of the company can include human resources, property of all types, confidential information, financial resources etc. The above-mentioned resources are located and stored in buildings and other units, such as warehouses and offices. These objects are the most vulnerable places and hence have to be properly secured.

The loss or damage of such resources could manifest itself with the following negative impacts for organization:

- Substantial material harm;
- A situation of threat to the life and health of the personnel;
- Spread of the confidential information or trade secrets.

Each of these impacts can become a source of problems to a company and even in severe cases lead to a bankruptcy of an enterprise. The degree of protection or level of security in general is evaluated by assessment of the controls between the protection asset and the threat (Firesmith, 2003).

Finishing up the discussion about security concept it can be said, that security is complicated and comprehensive object, which examination is essential in a plenty of areas.

Consequently, every organization under current market conditions is constrained for provision of security. Notwithstanding that each company has its own peculiar properties and environmental or industry limitations, some common features and functions of security systems can be founded out. Company of any kind performs functions of planning, organizing, developing, controlling and stuffing security as a part of security system. During security system implementation or rationalization organizational specifics should be considered in order to search out the best security solution for achieving corporate and business goals. Security management should be harmonized with business goals of organization and act as furtherance of their achieving (Briggs, Edwards, 2006).

Understanding the necessity of security precautions is vital for the successful operation of the organization. Failures in risk assessments and lack of attention to the potential threats may cause difficulties for organization down to bankruptcy. Companies with effective system of security can keep themselves out of unforeseen costs. In addition to it balanced security system gives to company some other advantages such as steadiness of inventories, defense from competitors' attacks, employees' loyalty etc. (Firesmith, 2003).

For the purposes of this thesis, the term "security" will be defined as the state of protection against threats, and the threats will be identified as economic losses only. The definition will be further narrowed down in section 1.3 to reflect the specifics of the retail industry. In order to assess security, the term security level will be used, because it allows to compare different business entities and to see by how much one business entity differs from another in terms of security. Several related concepts, such as threat, risk, impact, security system and secured object were also explained in this chapter.

## 1.2. Business entities' security system fundamentals

Organizational or otherwise known as corporate security strives for identification and mitigation of any situations and factors that threaten the steadiness, working efficiency or activity of the company. Corporate security notion joints all functions of security enforcement within the organization.

Characteristics of contemporary business environment further explain the role of security in organization. Market oversupply forces companies to take new risks; globalization changes the subject matter of business processes; recent forms of business activities produce an unnecessary pressure on companies and force them to accept new responsibilities in order to qualify the market requirements. Meanwhile the threats grow more and more complicated and multifarious. Certain threats such as organized crime or information security are network, fractal and trans-phenomenal, what makes them substantially uncontrolled.

All these matters of fact broaden and deepen the sphere of organizational security. Organizations are in the process of searching for advanced methods and instruments of security enforcement and risk management. Interplay between security and organization could be encapsulated in the range of characteristics (Briggs, Edwards, 2006):

- The true purpose of organizational security system consists in raising employees' awareness of security through often-performed and routine practices rather than guaranteed security;
- Security system should be in operation with organizational social network as against acting in a standalone mode;
- Security enforcement is meant to be an instrument of managing risks by preventing their adverse effects and taking them if necessary;
- Security system should be configurable and opportunistic on account of meeting changes during the process of organizational development;
- Activities on security enforcement are carried out both on strategic and operational levels of the corporate management;
- Justification of security system operations comes from its basic necessity and is driven by business intuition, expertise in communication and human resources management.

Basic kinds and forms of security are generalized for all types of organizations and other types of secured objects, regardless of their objectives. Sylvie et al. (2013) classifies security into three categories: "*physical, personnel and information security*". However, in practice all three are interconnected and must be thought of in a holistic manner.

Physical security corresponds to the range of practices that are developed in order to forbid illicit access to the resources of all types and secure them from losses and damages. The variety of different actions that are contributing to harm exists, such as espionage or theft or even terrorist attacks. The measures of physical security enforcement normally include several levels of interdependent systems – closed-circuit television surveillance (CCTV), protective barriers, access control, guards etc. Physical security systems are aimed on keeping from interruption, disclosing unauthorized intrusions and offenders and orchestrate relevant event responses. Listed functions are exercised through the usage of various security instruments – mainstream examples of them are warning signs, deterring from intrusion, alarms and CCTV, recording the process of intrusion, security guards, intercepting the intruders (Garcia, 2007).

Design of physical security system depends on the threat level and multiple environmental factors. In the course of developing physical security measured associated costs should be entertained consistently with organizational issues and any social and legal matters. Physical security system of prison would be inappreciable and redundant in the office, but the construction principles are identical.

Conceptualizing of physical security can be done through the classification of the levels. Layering of physical security system is performed according to the circumstances and organizational needs. There is no consensus on the criteria of leveling the physical security. Fennelly in his paper comes forth with five levels of physical security, varying from minimum to maximum security (Fennelly, 2016). Hierarchical arrangement of the physical security levels is pictured by Table 1.1

Minimum security system is forbidding unauthorized activity relative to the secured object. Minimum security level is provided by simple efforts such as equipping regular doors and windows with primary locks. Low-level security system in addition to forbidding unauthorized activity is detecting some abnormal environmental occurrences. Simple physical barriers on this level are complemented by security lightning, high-security locks and alarm system. To medium security enforcement existence of advanced alarm system, heavily protected physical barriers and security officer is peculiar.

Such security level allows the estimation of intrusions as well as detection and obstruction. High-level security system is bidirectional – such significant measures are instrumental in detecting, assessing and preventing not only external but internal security violations. This level of security is proposed to use a great number of state-of-the-art technologies, services of qualified guards and cooperation with local police and emergency response organizations.



Table 1.1. Levels of physical security Source: (Fenelly, 2016)

Maximum level	<ul style="list-style-type: none"> <li>• On-response force</li> <li>• Sophisticated alarm system</li> </ul>
High level	<ul style="list-style-type: none"> <li>• CCTV</li> <li>• Perimeter alarm system</li> <li>• Highly trained armed guards with advanced communications</li> <li>• Access controls</li> <li>• High-security lightning</li> <li>• Local law enforcement coordination</li> <li>• Formal contingency plans</li> </ul>
Medium level	<ul style="list-style-type: none"> <li>• Advanced remote alarm system</li> <li>• High-security physical barriers at perimeter, guard dogs</li> <li>• Security officer with basic communications</li> </ul>
Low level	<ul style="list-style-type: none"> <li>• Basic local alarm systems</li> <li>• Simple security lightning</li> <li>• Basic-security physical barriers</li> <li>• High-security locks</li> </ul>
Minimum level	<ul style="list-style-type: none"> <li>• Simple physical barriers</li> <li>• Simple locks</li> </ul>

Maximum level of security provides a means of neutralizing all the types of unauthorized activities relative to secured object. In contradiction to previous levels maximum security enforcement imposes the occurrence of proper on-response force on twenty-four-hour alert. Implementation of such a system is a wise measure for military bases or nuclear facilities rather than commonplace business organizations (Fenelly, 2016).

To gain a better understanding of physical security tools its components should be considered. Basic components of physical security system are:

- Deterrence methods;
- Intrusion detection and electronic surveillance;
- Access control;
- Security personnel.

Deterrence methods stated another way is crime prevention through environmental design (CPTED). The target of physical security of this sort is advertising of intruders about their actions' consequences and a payment for keeping them from the attack. CPTED makes for approach to security enforcement through affection on the trespasser. Discouraging the unauthorized activity underlies the foundations of the CPTED design, while methods vary from simple to all-encompassing (Fennelly, 2016). The most commonly used deterrence methods include fences, warning signs or stickers, height restrictors and barriers, security lightning etc.

Surveillance in terms of security corresponds to the process of threat monitoring with the aim of preventing the intrusion. Intrusion detection and surveillance could be provided by means of specialized technical equipment, such as alarm systems and closed-circuit television cameras. Alarm systems serve the purpose of other security system components triggering. Without distinction of alarm system characteristics its usage requires formulation of some scenario, which describes proper actions against a backdrop of emergency or intrusion. Video surveillance is appropriate form of security enforcement, when disposition of cameras keeps highest possible scope and all the insecure points. Overarching goal of the CCTV usage is the creating the possibility of the fast response along with recording capabilities instrumental for intrusion analysis and verification.

Access control means are helpful for monitoring and controlling of the traffic near or within the secured object. Access control protective equipment can be mechanical or electronic. Employment of mechanical access control systems in the current context is inadequate for security assurance. Mechanical keys are subject to loss and counterfeiting. Electronic access control systems now appear to replace mechanical locks because of the fact they provide a better means of preventing unauthorized access and superintendence. Besides access control systems implementation there exists a necessity of access policies development – rules, setting the limits of access to the different objects of security for various groups of people.

Security personnel are at the forefront of the any physical security system. Electronic and machinery use is impossible without human participation. Staff involvement in the security process is essential for performing functions of security process administration, responding to alarm systems signals, monitoring and militating to the treats on a direst basis (Reid, 2005).

The following table (Table 1.2) lists the most common forms of physical security components and describes their subject matter. Typically a number of security methods are used simultaneously with a view to creating of comprehensive and complete physical security system. A set of methods and tools is specified depending on peculiar qualities of the secured objects and projected expenditure.

Table 1.2 Forms of physical security components (Author, 2017)

Physical security component	Forms	Description
Deterrence methods	Physical barriers	Surface security level, protecting from external threats by intercepting or at least delaying; also holds psychological meaning in creating the impression of access difficulty; normally located along the perimeter of the secured object (Talbot, Jakeman, 2011)
	Natural surveillance	Outer spaces around the secured object, that provides a means of better seeing and controlling unauthorized actions; makes impossible to achieve the secured object unnoticeably
	Security lightning	Illumination of the secured object, which fulfils similar function with natural surveillance; account must be taken of intensity, power supply and allocation of security lightning – low-intensity hardly accessible furnished with emergency lightning source light fixtures are preferred (Kovacich, Halibozek, 2003)
Intrusion detection and electronic surveillance	Alarm systems	Notification means, working in a concerted effort with physical barriers and security personnel; intended to alerting security personnel about unauthorized interaction with secured object; typified by motion or contact sensors
	Video surveillance (CCTV)	Technical equipment, dealing with filming and recording of the circumambience for purposes of historical data analysis and intrusion recognition; demands for human participation in real-time mode in order to enable timely intervention to the situation
Access control	Mechanical access control	Gates, doors, locks and other means of impeding access to the secured object; underperformed virtue of electronic access control systems entrée
	Electronic access control	Substitute of mechanical locks by means of computer technology; allows to administer a great number of users and access points using the resources of one control center
	Identification systems and access policies	Procedural form of access control, helping to define a filter for access permissions; typically underpinned with mechanical or electronic access control systems
Security personnel	Security guard	Human element of physical security system, that ensures the work of all other components and makes provision for prompt response

Personnel security in the context of organization refers to the safety of organizational staff, including not only life and health security and protection of the rights of employees but also the degree of organizational protection from adverse employees' actions. According to Grigoryeva personnel security can be defined as personnel's protection from external and internal threats (Grigoryeva et al., 2016). The ultimate goal of the personnel security measures is laying the groundwork for human resources management, which, in turn, contributes in labour productivity increase and overall organizational effectiveness.

In the light of organizational effectiveness personnel security enforcement corresponds to prohibiting of negative effects of external and internal environmental factors on employees by minimization of related risks and threats. Security of organization in general heavily relies on the personnel security treatment and supporting means of security enforcement. Fears connected with personnel could be incidental to either life and health danger or threats for intellectual potential and job relations in broad terms. Employee participation in all organizational activities and processes attaches importance to the complete list of personnel risks.

Personnel security of organization depends on management intentions regarding human resources. Management process should be sensitive to personnel's actions and influencing on them factors by the reason of the human impact on the security. Personnel risks translate into organizational threats. Threats to the personnel security can be divided into two categories – external and internal. An example of external threats to personnel security would be brain exodus, low labour-market skills of employees, deficiency in highly qualified specialists etc. Different types of addictions or absence of corporate culture and motivation may serve as an example of internal personnel threats (Egorova et al., 2013).

The main causes of personnel risks emergence from the point of employees' and environmental characteristics may be following (Grigoryeva et al., 2016):

- Qualification asymmetry of fellow applicants;
- Professional imbalance of demand and offer in labor market;
- Unclear moral and value stances of personnel;
- Low level of employees' qualifications;
- Low level and quality of living conditions.

Insightful analysis of peculiar properties of personnel security in the context of organizational activity gave an option of specification and classification of factors making contingent on the threats emergence. Instance of threats to personnel security of organization constitute a danger for its interests realization. Figure 1.1 depicts the list of influencing factors on personnel security in organizational context, divided on the grounds of relation to the company and controllability.

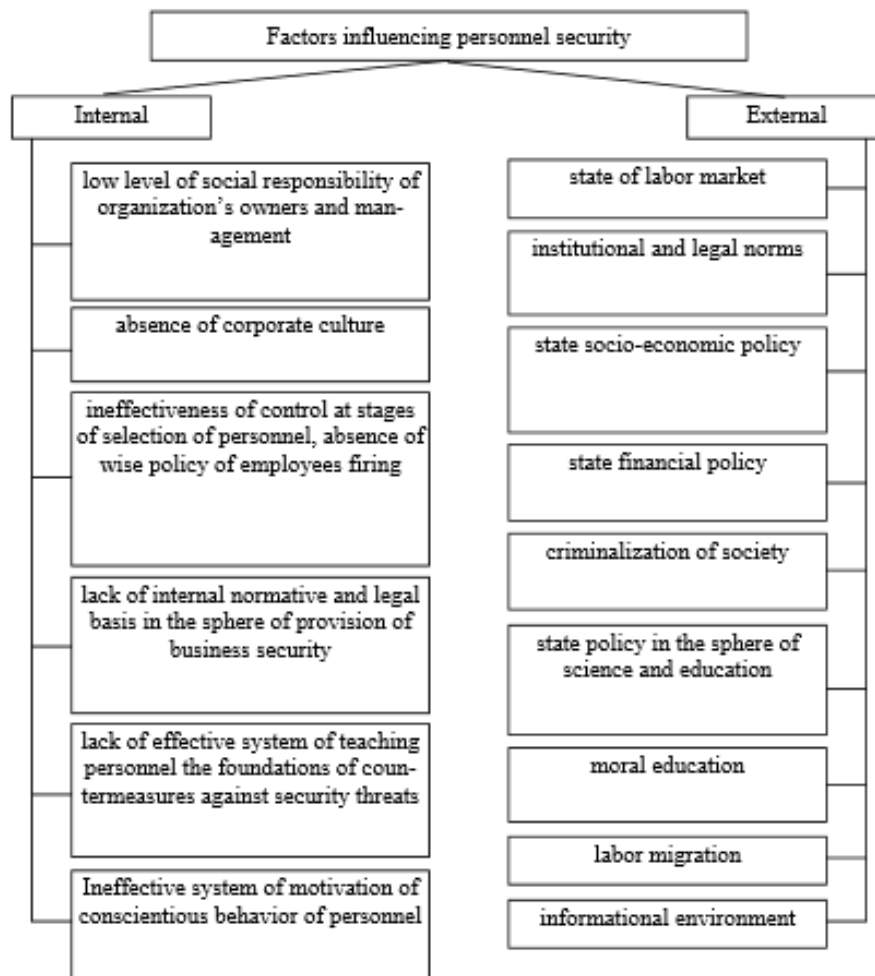


Figure 1.1 Factors affecting personnel security in the context of organization  
(Grigoryeva et al., 2016)

Awareness and consciousness of factors influencing potential threats to personnel security creates the possibility for organization to manage with dangers and minimize personnel risks. Organizational system of personnel security should be sensitive to specified above factors and supported by computations and documents. Personnel security system development should focus on compilation of appropriate methods of personnel management and protection. Personnel security enforcement should encircle all the periods of contact between organization and employees from hiring to resignation.

The degree of organizational security is evaluated by the reference to the weak links in security system (Lincke, 2015). Commonly believed weakest component of any system is human factor – due to this precise reason organization should place special emphasis on personnel security to strengthen the bottleneck of the whole security system.

One of the key goals of the personnel security system is providing staff with the information about security policies and understanding of them, outlining their responsibilities in the sphere of security and implementing of security functions performance. The other equally

important aim of personnel security is prevention of the fraudulent activities. 70 percent of information theft within the organization is the responsibility of dismissed employees or some of them who are planning to leave (Verizon report, 2013). Negligent entrustment to the employees is problem of the frequent occurrence. Organization with balanced personnel security system can prevent or avoid such threats by supervision of the staff behavior and accurate allocation of responsibilities and access rights.

Split of responsibilities is one of the most efficient methods of security enforcement and defense from employees' dishonest actions. Whereas each employee plays the certain part with restricted access rules security breach is rendered substantially out of the question or at least monumental challenge. There becomes no way to attack the security system using the resources of one employee. Access guarding and restriction can be quite easily done in the present context by implementing the computer system with authorization and access control.

If the segregation of duties is impractical due to organizational specifics and the specific of the goals of organization, several other measures of preventive and deterrence control could be introduced (Lincke, 2015). Such measures and techniques provide an opportunity of keeping organization from fraud at the hands of personnel and external threats by the same token. Figure 1.2 gives the insight into the means of personnel security in organization, dividing them into two groups.

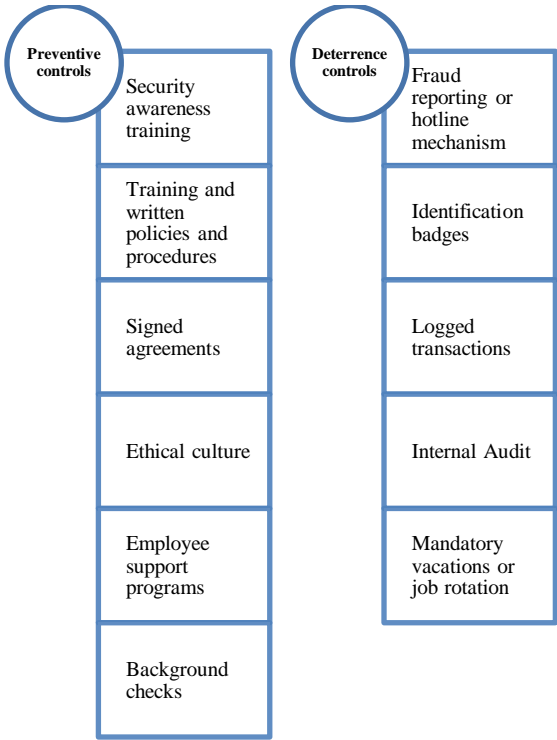


Figure 1.2 Means of personnel security in organization, (Lincke, 2015)

Instruments of preventive control are targeted at the avoidance of potential hazards to the security. Security awareness training corresponds to the explanation and reasoning of

organizational security policies or procedures as well as their regulatory compliance. During these occasions employees of the company are qualified in safety precautions such as password generating, computer systems usage, operation techniques meeting the requirements of security enforcement etc. Written policies and procedures of the personnel security enforcement encapsulate job standards. Signed agreements refer to accordance of staff with organizational security policies and requirements. Examples of such agreements could include:

- Code of conduct – description of general principle of ethical conduct for employees;
- Acceptable use policy – rules for accessibility of organizational data and internal information;
- Privacy policy – behavioral rules regarding confidential information of the company etc.

Ethical culture of the organization ensures compliance of security requirements from the moral perspective. Employee support programs are intended for staff problems' solving in order to eliminate repercussions in the area of human resources management. Background checks are applicable for employees handling secured identifiable information or somebody with advanced access rights (Lincke, 2015).

Deterrence control measures are aimed on detection and identification of intrusions. Fraud reporting or hotline mechanism is about opportunity of any employee to signal about eventual fraud to internal security department or an independent security agent. Sometimes such mechanism includes material reward for claimants. Identification badges allow distinguishing between employees, partners and visitors of the organization. Handing out and exploitation of identification badges should be under strict control. Logged transactions provide the opportunity for review some important or unauthorized occasions. Usually logging is used for financial or monetary transactions, along with this some of them should be pre-authorized by higher-level managers. Internal audit procedures are effective means for fraud detection and with the view to ensuring compliance (Lincke, 2015). Job rotation and mandatory vacations help in recognizing unauthorized or nonconforming activities.

Information is among key assets of an organization, that's exactly why nowadays information security is considered to be the crucial element of organizational security system. In the current business landscape, the information becomes more and more important. Information is "any organized documentation or data". Information can be present in the organization in a range of forms and some forms of information storage are more risky than others. Previously, the primary focus was on securing the physical assets, while nowadays with the development of various means of information transmission and storage, such as internet and cloud, the focus of

information security management has shifted (Turban et al., 2012). Haufe et al. (2016) state that cost-benefit analysis of the security strategy is among the most important considerations in the security strategy design.

One type of information that has to be properly protected is information about the customers. Employee awareness and training programs play a significant role in protection of sensitive customer information. An important way to protect this information is education of the employees on the potential threats that is associated with the data that employees have access to (McCrohan et al., 2010).

Nowadays Internet is becoming more and more prominent in daily lives, affecting multiple routine activities such as information search, communication, banking, etc. Because of this, online security now is among important issues for companies. A breach could lead to significant direct and indirect losses. Perceptions of online security are also important, because if they are negative they could lead to a decline in overall trust to an organization's online services. Because of the significant consequences of online security breaches, companies invest money to install protection measures to secure access to systems (Tam et al., 2010).

Firewalls, authentication systems and other methods are being used to protect the systems. However, even though these technical measures are being implemented, the protection level is far from perfect because companies often neglect the key element of their systems – the user. In general, companies still use password-based systems in order to control the access to the systems. Thus, it is important to focus the attention on users, because their behavior in many ways determines the security of the system. Password-management techniques are of utmost importance when it comes to user behavior and security of the system (Tam et al., 2010).

According to widely accepted guidelines, the password should be memorized, only used for one year, not written down and randomly assigned. These requirements for password reduce users' productivity because they challenge the cognitive abilities. Hence, knowledge about these guidelines is not always accompanied with the good password management. One of the reasons for this password mismanagement is users' overly optimistic attitude towards the most likely scenario of the future. Users tend to think that although online security breaches are a huge problem, it will not happen to them. This optimism is a likely explanation for common mismanagement of the passwords (Campbell, 2007). Even IT professionals fall into the category of users who mismanage their passwords. For instance, according to a recent survey of IT professionals, 40% write down their important business network passwords (Millman, 2006). This practice of writing down passwords may lead to poor security. Another example of mismanagement is not changing the default passwords set up automatically by the system.



Additionally, when the default password is being used it is most likely randomly generated and therefore difficult to memorize. This in turn increases the likelihood of password being written down, which, as described above, is not an example of good password management. User awareness programs, including training and education are being suggested to minimize the password mismanagement practices (Bresz, 2004). The researchers argue whether the online security should be the responsibility of IT departments, or whether it should be a responsibility of the user as well. Responsible behavior also sometimes is being regarded as an obstacle to the daily tasks. Psychological principles may be used to better understand behavior patterns related to security, because human aspect of security is important. Motives behind common password management behaviors were examined as well as the security-convenience trade-offs by Tam et al. (2010). The five password-management behaviors identified by the author of the research are:

1. First time password choice
2. Change of the password
3. Allowing someone else to use a password
4. Taping the password close to the laptop
5. Sharing the password with close friends or family

The first two behaviors are neutral in their nature, while the rest of the password management behaviors are the ones that managers would like their employees to avoid. According to this study, most users are able to distinguish a good password from a bad one. Also, because it is convenient, 42% of the users are willing to share their passwords with someone they trust. It is also important for users that a password can be easily retrieved, because forgetting password is common.

Additionally, users desire to have passwords that can be easily remembered and because of that they tend to choose weak passwords or sometimes even reuse old ones. Privacy security concern was mentioned more times than any other. Exposure of the information to a third party was the second top mentioned concern among the users. More harmful issues, such as fraud were mentioned less frequently which is quite surprising. The study revealed that users in the majority have the knowledge of what constitutes a secure password, however it is associated with losses in convenience, which the author calls “security-convenience tradeoff” (Tam et al., 2010). The author states that more education on password management would not necessarily lead to a better password management behavior, because the users surveyed were aware of the fact that some of the behaviors they exhibited was wrong, but they still chose to pursue such behavior because of its convenience. In the first two behaviors, which are as stated previously rather neutral, users also mentioned concerns about both security and convenience. It is interesting to

look at what can possibly affect a user's willingness to trade convenience for security. The study has concluded that the type of account as well as the time frame of password selection process both affects the security-convenience tradeoff resulting in certain password quality, as shown in Figure 1.3.

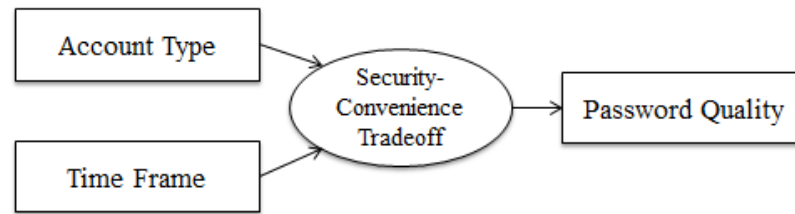


Figure 1.3 Information security-convenience tradeoff, (Tam et al., 2010)

Security awareness programs are among the crucial aspects of security design. Employees should be made aware of how their actions impact overall organizational survival (Guynes et al., 2012). Awareness programs should be created for the purpose of training every employee who is in contact with the organization's information. They should ultimately adjust any behavior that might potentially endanger the information security of the organization.

The aim of such programs is to create enough knowledge among the employees for them to not only adjust their everyday behavior but also to respond more timely and accurately in the cases of notifying suspicious signs in the information systems they work with. The behavior of users can be adjusted if the awareness program is specifically tailored to non-IT personnel. It is also necessary to tailor training to the group of individuals, their work environment and routine tasks. This will make the training more interesting and relevant for employees, creating more motivation for them to learn and memorize the material (Guynes et al., 2012).

Table 1.3 Objects of protection categorization, (Russian legislation)

<b>AI</b>	<b>AII</b>	<b>BI</b>	<b>BII</b>
special importance highly dangerous life-sustaining fine jewelry stores weapons warehouses	storages of monetary assets storages of fine jewelry secret documents storages	retail stores of various size and format technical documentation storages	stores that sell computers, cameras, fur, cars, and alcohol

Fundamentals of the business entity security concept were described in this section and the three key elements of every security system were identified to be physical, personnel and information security. Then, the protection mechanisms used in the security systems, such as alarm, surveillance and security guards were described. Each component of security system of the business entity was described in detail and the next section will reveal the specifics of the

security system functions, structure, maintenance and assessment in the context of the retail industry.

The objects of protection are classified into four groups, according to the Russian legislation, in particular Ministry of Interior Directive N78.36.003-2002. The groups are called AI, AII, BI and BII. The groups' shortened description is presented in Table 1.3. According to this categorization, retail stores fall into BI category.

### **1.3. Retail outlets' security system specifics**

Mittal et al. (2011) cites a number of challenges that organized retailers face. The challenge factors cited are technology, logistics, skilled workforce, consumer behavior understanding, variations in customer demand, and several more. For unorganized retailers the challenge factors included competition from organized retailers, operation costs, logistics issues, and retail shrinkage. As a part of the study, the survey was conducted. It was based on data collected from 50 managers of organized and 50 managers of unorganized retail stores, whereas the sample was chosen through convenience sampling techniques. According to this survey, retail shrinkage is among top three challenge factors for organized retailers, along with competition from unorganized retailers and logistics issues.

In retail, consumers' needs drive purchase decisions and hence must be analyzed. The recent developments in technologies, business models, and big data analytics shape the future of modern retail landscape. Innovations change the retail landscape in many ways. For example, targeting consumers has become easier with the advances in technology. Also, the decision making process of what product to buy is influenced with technological advances. Now retailers can have better insights into what kind of consumer is making a certain purchase (Grewal et al., 2017). Several authors have contributed to the investigation of the role of impulse buying. They proposed that purchases could be stimulated right on the point of sale, rather than planned before. This stimulus could be directed towards profitable product categories. Over the last twenty years the strategic focus has shifted from advertising and other traditional marketing methods that were meant to create awareness among buyers to in-store marketing methods, such as promotion mechanism with the aim to impact consumers' decision on the point of sale. Retailers have allocated larger budgets for this stimulus of unplanned purchase techniques. It was researched that in Italy two out of three decisions about purchasing are done in the store. However recently consumers became less prone to make purchase decisions in the store and became more inclined towards thorough preparatory planning, which reduces the inclination towards impulsive behavior in the store (Bellini et al., 2017).

Shoppers experience in the store is one of the key drivers of sales. Retailing today has a wide variety of new technologies that may be implemented, such as self-checkout option, mobile apps, or smart shelf technologies. The way the shopper perceives the experience with a particular technology affects the potential effect of the technology implementation in the store. Therefore the shoppers' perspective on the product should be taken into account at all times when planning strategic decisions (Inman et al., 2017).

Beck (2002) discusses the notion of shrinkage in retail. The author states that shrinkage may be defined in different ways. More precisely, the definition of shrinkage may either include or exclude the losses occurring in cash. A broader definition involves both stock and cash losses, and any so-called indirect losses, such as the sale of counterfeit products or the subsequent sale of the stolen goods. In any case, the term describes losses that occur throughout the processes of producing, distributing and selling goods to consumers. Variations in the exact figures of shrinkage in retail per country occur among different studies because of the different definition of the shrinkage. As stated above, the major difference among definitions arises because of either inclusion or omission of cash losses in the definition of shrinkage.

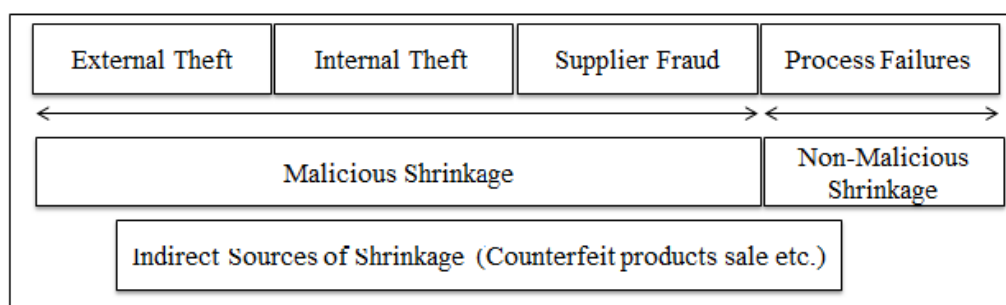


Figure 1.4 Schematic shrinkage definition (Beck, 2002)

The term encompasses a number of events, all of which could be categorized into two categories: malicious and non-malicious events. Both have a substantial impact upon the overall profitability of an organization. The two categories imply different preventive measures, however sometimes the measures for tackling the problems of malicious and non-malicious shrinkage do overlap. The definition provided by Beck (2002) is based upon categorization of shrinkage based on the source of event occurrence. The author defines shrinkage as a combination of both cash and stock losses, which results from one of four categories: external theft, internal theft, supplier fraud and process failures. Other contributions to shrinkage come from the indirect sources, such as stock-outs, counterfeiting and selling of stolen goods, according to Beck (2002). The schematic definition of shrinkage is presented in Figure 1.4 .

In the study done by the Global retail theft barometer in 2015, the four major sources of shrinkage were investigated. The study has found that internal theft accounts for 39%, internal theft accounts for 38%, administrative errors (process failures) account for 16% and supplier

fraud accounts for 7%. The Global retail theft barometer is a study on shrinkage trends conducted in 24 countries across the globe. It is done by Smart Cube company in collaboration with the global loss prevention expert Ernie Deyle. The study was done through in-depth phone interviews and the written survey interviews among over 200 retailers. This study is performed in order to identify the trends in the global shrinkage issue, investigate the leading causes and analyze the most effective methods of loss prevention.

Bottom of basket loss is a special type of loss which occurs when the goods are put on the lower tray of the shopping cart and the cashier overlooks the items, which leads to the items not being paid for. This type of loss can occur both intentionally and unintentionally, but either way it results in reduced profit margins. One of the suggested ways to combat such type of loss is to use a special system that would alarm when anything is placed on the lower tray (Dulyakorn et al., 2011).

The loss prevention in retail consists of many activities. For instance, losses have to be investigated; store staff has to be educated on various types of risks that occur because of theft or fraud. Moreover, it is important for an organization to learn how to protect itself against cybercrime. Often, the retail establishment delegates these functions to a specific loss prevention department. This department then manages physical security by equipping the store with various theft deterrents. Typically, the loss prevention department works together with the human resources department in order to assure maximum response towards losses (DiCarlo, 2017). Pretious et al (1995) talks about retail security and discusses methods of retail security management. The focus of the article is physical and procedural methods that are being used. Also, authors evaluate the perceived effectiveness of the methods from the viewpoint of management.

Indeed, retail loss prevention is a distinct direction of managerial effort. Fernie et al. (2015) identifies three ways of combatting shrinkage:

1. Human
2. Mechanical
3. Electronic.

The examples of each category of loss deterrents are presented in Table 1.4.

Theft and resulting shrinkage are major problems for retailers (Koh et al., 2003 and Knežević et al., 2016). This implies that security is a great concern for retailers. Even though the investment in new loss prevention technologies is heavy, shrinkage is consistently a problem that is difficult to resolve and is a significant cost to retail industry. Globally, shrinkage is estimated to be \$278 bln per year (Beck, 2010).

Table 1.4 Examples of loss deterrents (Fernie et al., 2015)

<b>Human</b>	<b>Mechanical</b>	<b>Electronic</b>
Employee screening	Locks	EAS tags
Audits	Mirrors	CCTV
Risk assessments	Lockers	Secure payment applications
Rewards	Security doors	Burglar alarms

Greggo et al. (2016) states that watching of the actions and the behavior of the customers is the key to identifying an external theft. Shoplifters are not characterized with same traits; basically anyone in the store can turn out to be a shoplifter. Shoplifters are classified according to their expertise into four categories: professionals, “thrill seekers”, amateurs and juveniles. If the professional shoplifters steal for the income, the “thrill seekers” steal for the emotional feeling of rush that they get from it. This type of shoplifters reveal themselves more easily with certain behavior that shows the nervousness, such as biting a lip or gazing around in order to see who’s currently looking at them. This type of behavior could be more easily noted by the security guard who watches the screen of the CCTV. The third category, amateur shoplifters, are much harder to catch because they behave very calm up until the action of stealing, because they do not decide on that in advance. Juvenile shoplifters typically do not steal expensive goods, rather targeting small toys or candies.

One of the prevention measures for a store is having personnel in the store trained so that they can recognize the signs in behavior of a customer, generally attributed to theft behavior. These behavioral patterns include paleness, avoidance of the store employees trying to be left alone, wearing clothes not suited for the season, and so on. Overall, when merchants are focused on behavioral patterns and body language rather than on social status or nationality, they are more likely to spot a potential thief (Greggo, 2016).

Two types of method exist in retailing for combatting the problem of external theft: preventive measures that, in essence, minimize the opportunity for shoplifting and increase risks of being caught while stealing, and second type of methods – catching the shoplifter during the act of stealing methods. Among the preventive methods there are electronic article surveillance (EAS), which can use either acustomagnetic or radiofrequency technology. The acustomagnetic type of EAS uses a tag filled with metal in order to be detected by special sensors. The radiofrequency type uses a different technology, an attached diode, which is also detected by sensors. The sensors could be placed in the ceiling, floor, or doorway (Greggo, 2016).

The author stresses the importance of personnel training in complement to the systems installed. The responsibility of the store personnel lies in controlling over the goods as well as

responding to the EAS system after its activation. Courteous treatment of the customer in such situations is essential. Some items may falsely activate the system, such as some pacemakers and various types of cell phones. The store personnel should remember that the most important feature of the system is its deterrent function. Together with EAS systems, stores nowadays begin to engage camera systems that can record the malicious activity. Not only it provides evidence for the police in the event of theft, but also it serves as a deterrent (Greggo, 2016).

Various types of cameras are being used: analog cameras, internet protocol cameras, digital video recorders and network video recorders. The major difference in cameras is the clarity of the picture. Some cameras use high-speed internet for connecting the equipment with the office in order to be viewed remotely. Another feature that makes these types of cameras different is the amount of information it can store. Common size of DVR hard drives is 160 to 250 gigabytes, allowing to store from one to 3 months of recorded video, given that the cameras have the motion detection feature and are set up to record in motion only (Greggo, 2016).

The number of cameras varies depending on the area of the sales floor as well as on the number of departments that have to be covered. The budgets, as well as the proposed return of investment play the role of constraint in the number of cameras installed as well. In general, this is done through comparison of the cost and expenses to the amount of money that can be saved by using such system. Apart from reduction of stock losses, the video recording can also be beneficial to the store managers by providing detailed information on the number of customers and missed sales opportunities, as well as benefit indirectly through the avoidance of certain types of lawsuits. If the cameras are set up to show the customer on a public view, creating an awareness that the customer is being watched (Greggo, 2016).

Another major cause of shrinkage, *internal theft* is hard to detect and uneasy to cope with because of the degree of trust that rests with employees. Moreover, oftentimes the managers are involved in the process, which makes it even more difficult to detect. There is a number of ways that employees might use in order to steal from a retailer, such as taking cash from the till, stealing from the stockroom, and including free items in collusion with customers (Ferne et al, 2015).

One of the organizational countermeasures of employee theft is *reward systems*. Both monetary and nonmonetary means are being used by companies in order to create successful reward system. Strategic use of rewards helps to attract, retain and motivate the staff. However reward system design must be tailored to company specific organizational strategy and culture. Reward system has many elements, although it is necessary to mention the most common ones. They are wages, bonuses, vacations and health insurance (Holston et al., 2015). Other means include creation of a friendly work environment, a sense of job security, and recognition of key

employees. These elements promote self-esteem of employees and helps gain loyalty to the company. Creation of a supportive work environment that makes employees see opportunities for advancement and development is valuable method of rewarding (Milkovich et al, 2017).

Increasing employee loyalty is a comprehensive task. The primary reason people work is to earn money and therefore monetary based rewards is an integral part of a successful reward system. In addition to the base pay, companies often times give out annual bonuses, which can be seen as a substitution to merit pay. Sometimes companies also reward for group performance above a certain standard level of performance with a profit sharing plan.

When a company designs nonmonetary elements of its reward system, it should incorporate several considerations in its design. First of all, the reward should be presented publically or be a tangible gift that can be easily displayed to the group. Another thing to consider when giving out rewards is the frequency of these events. In order to remain important to the employees the reward should not be given out too frequently. Additionally, the selection among potential recipients should be considered a fair process for the credibility of award. Then winning employees will be seen as role models for the group and promote a healthy competitive environment among the employees. Lastly, there should be a correlation between the reward and the cultural values of the organization (Holston et al, 2015).

Another countermeasure against internal theft is *employee screening* before hiring. A number of various deceptive practices exist on the stages of resumes submission, applications submissions and employment interviews of the employment process. Such practices include misrepresentation and fraud. Lying about the previous criminal history, work experience and degrees held is not necessary illegal but such occurrences may be minimized with an effective employee screening practices (Ficht, 2011).

Another practice that is used against internal theft is *mystery shopping*. Mystery shopping is a special technique that is used by retailers to evaluate intangible service experiences. Measuring the quality of intangible service experience is a challenging task otherwise (Ford et al., 2011). The goal of mystery shopping is to collect information about the shopping experience as well as the behavior of the employees in order to benchmark and identify areas of improvement. The information gathered by mystery shopping tends to be more objective than information gathered by surveying regular customers and also this method is more cost-effective (Mattsson, 2012).

Modern retailing is becoming more and more complex, due to globalization of goods' manufacturing and distribution. The global consumer now is used to the availability of a vast variety of goods that often were manufactured far away from the point of sale. The complexity of the manufacturing, distribution, and sale processes has resulted in the problems associated with



the complex nature of it and the vast variety of processes that need to be recorded properly (Beck, 2002).

However, oftentimes the processes are not being properly recorded. Sometimes the issue is omitted linkages among information flows, other times the issue is in having the right products in the right place. Overall, such issues are called process failures or else paper shrink. Process failures constitute a significant cost for retailers for not doing them right. The major contributions to process failures are made because of errors in: outdated stock handling, reductions in price handling, stock damages handling, delivery, pricing, scanning, inventory check, product promotion, master files, returns handling, and transfers within the company (Beck, 2002)

#### **1.4. Hierarchic system of criteria of security system assessment**

In the figure 1.5 the hierarchic system of criteria of security system assessment is presented. The first layer of the hierarchy was developed in Section 1.3 through the analysis of scientific literature on the topic of security in retail. Each element of the first layer of the hierarchy corresponds to one of the original sources of losses. These five elements represent the threats that are the most common in retail industry and from which it is obligatory to be protected from.

The second layer of the hierarchy represents the classification also researched from the secondary sources and this classification is the division of the protection measures into organizational and technical measures. Initially, the classification was human, mechanical and electronic, but after speaking with the experts during the interviews it was concluded that mechanical and electronic classification is no longer relevant due to the fact that technology is constantly upgrading and evolving. Thus, nowadays almost all mechanical and electronic mechanisms of protection are not separated but rather combined into one, or at least share the elements of one another. Therefore it was decided to combine these two groups of criteria into one and to call it technical measures of protection.

The third layer of the hierarchy is the result of the in-depth interviews with the experts in the field. The experts were asked questions like “To your opinion, what are the most effective and commonly used organizational protective measures against internal theft?” Or “To your opinion, what are the most effective and commonly used technical protection measures against supplier fraud”. One of the significant differences in between the answers of the interviewees and the background information gathered through scientific literature research was that the RFID (radio frequency identification) technology is apparently not used in the context of Russian retail market, even though RFID technology and its advantages, applications, and disadvantages are perhaps the most extensively covered in the scientific community in various journal articles. Experts were additionally asked on their opinion on why this is happening this way and on why the RFID technology is not used in Russian market, and the answers were primarily related to the high cost of implementation of the technology. The only instance that the RFID technology is used currently in the Russian market is in the so-called test stores.

First three groups of elements represent the threats that occur intentionally and are maliciously conducted with the aim to steal. These elements include internal theft, external theft and supplier fraud. These three elements represent actions deliberately taken with the aim to steal from the retail stores. Protection against such actions is highly important. The rest of the elements represent two groups that cannot be called malicious per say, for instance the administrative errors or otherwise called process failures sometimes occur unintentionally and therefore are non-malicious. Cyber threats however, can be both malicious and non-malicious in nature. A vast range of non-malicious cyber threats related to password safety and actions of the employees exist. The four elements are discussed in practically every source of literature researched, but then there is the fifth element which only recently starts to gain attention, and that is the cyber security of the business entities. For some industries, such as banking, or hazardous manufacturing, the issue of cyber security is well known and well thought of. For retail industry, it still seem to be a newly rising concern with the stores not having a clear picture of how to combat the potential vulnerabilities in terms of cyber security. After the interviews it was decided to include the cyber security element in the hierarchic system of criteria of security system assessment. Later on when the weights were assigned, the cyber security received lower weight than other elements, because as it was already stated, it is a new concern for the retail industry.

The developed hierarchy has several levels. In order to assess the protection of the retail outlet from the internal theft, the following organizational measures were identified by the interviewees:

- *Reward system.* It may seem that monetary benefits will serve as a precaution against employee theft, however non-monetary benefits could serve as a precaution as well, or even better. Overall the effective reward system positively affects the security aspect related to internal theft.
- *Screening.* Employee screening before hiring is an important tool that serves as a filter of the pool of applicants. It helps employer to be confident in employees. The better the employee screening procedure, the more protection from internal theft the employer has.
- *Awareness.* Awareness programs, aimed at the increase of awareness in employees and customers typically comprise of banners in the stores, special trainings and campaigns. In stores with raised awareness the maintenance of security is easier.
- *Audits.* Security audits should be conducted as well in order to maintain the desired level of security. This is a tool for security level maintenance.
- *Mystery shopping.* Mystery shopping may reflect certain problems that are prevalent in the store and are not identified by other mechanisms.

- *Security team.* If the store has the security team in the store, which is formed specifically for the maintenance of the desired security level, it typically creates a basis for the certain security level.

- *Customer involvement.* Involving customers in the process of combatting the internal theft instances also serves as a tool that increases overall security.

- *Employee education.* Training and education of employees also yields results in the direction of security level maintenance.

- *Polygraph*

- *Collective liability.* Collective liability ensures the liability of the employees in the event of theft and serves as a precaution against such instances.

The following technical measures of protection against internal theft were identified:

- *Cashier control system*

- *Hours control system*

- *Access control system*

- *Video surveillance*

- *Burglar alarm system*

The following organizational measures of protection against external theft were identified:

- *Awareness programs.* Similarly as with the internal theft, awareness programs serve as a precaution against external theft as well.

- *LP Specialist.* Oftentimes loss prevention specialist is a required measure and a required expense (i.e. salary) for the maintenance of store's security at the desired level

- *Security guard*

- *Rapid response team*

- *Lawsuits handling.* The practice of handling lawsuits that may occur in event of thefts shows the stores readiness for such events.

The following technical measures of external theft protection were identified:

- *EAS.* Electronic Article Surveillance is one of the most common measures of protection that is implemented in retail. It is almost imperative for retail stores to have EAS system installed in the store

- *CCTV (Closed circuit television)*

- *Burglar alarm*

- *Mirrors*

Similarly, the factors were identified for the rest of the branches of the hierarchy. The complete list of the criteria of security system assessment is presented in the figure 1.5.

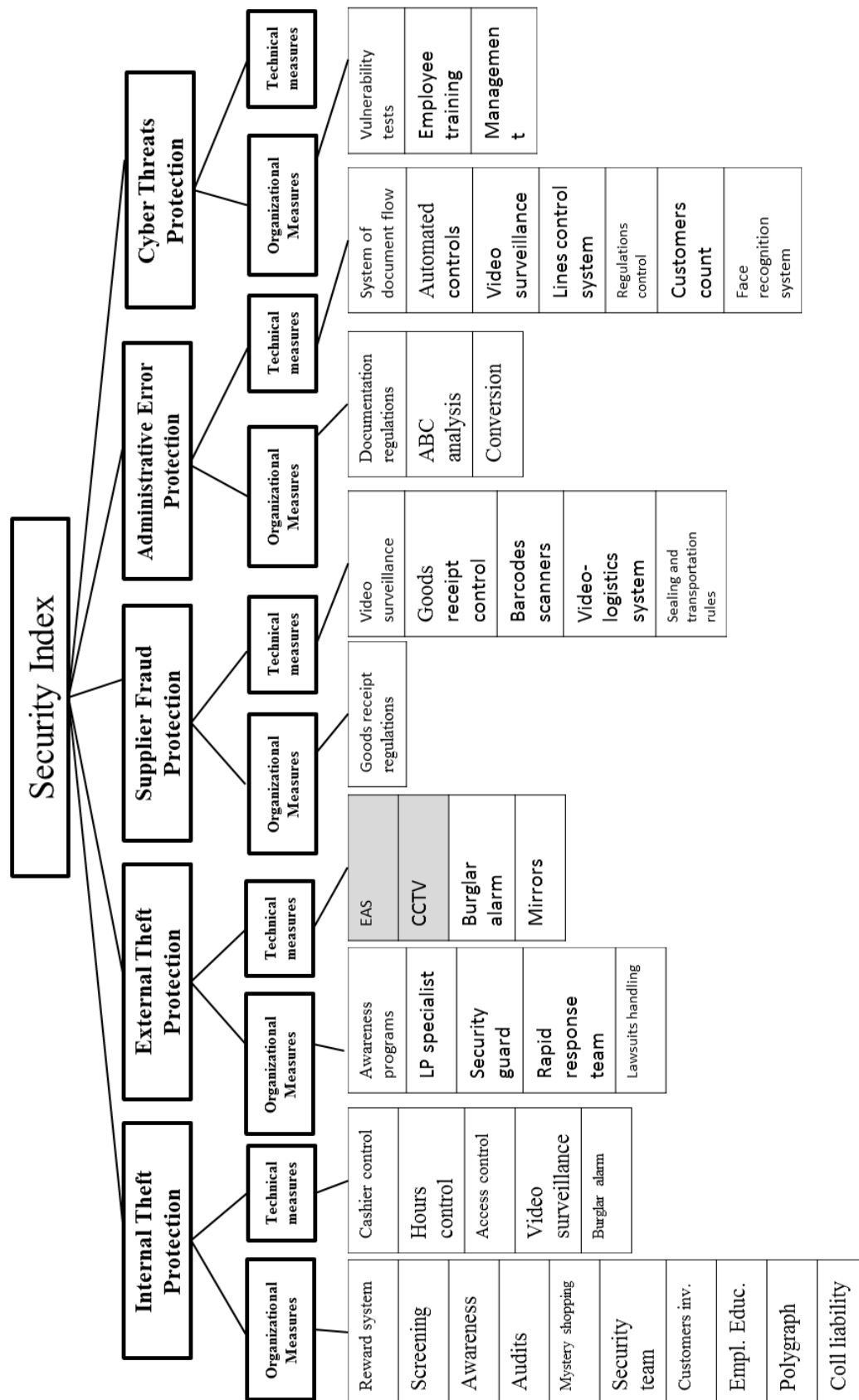


Figure 1.5. Hierarchic system of criteria of security system assessment (Author, 2017)

## **CHAPTER 2. SECURITY SYSTEM ASSESSMENT FOR RETAIL OUTLETS**

The aim of this chapter is to develop a framework of security system analysis for retail outlets on the basis of selected criteria and quantitative evaluation of the questionnaire results. First, the methodology will be discussed. In the second section of this chapter, the methods will be compared and contrasted in order to select the most suitable method for the solution of the problem of security system assessment. In the third section of this chapter, the framework development process will be documented.

### **2.1. Research methodology**

The research was conducted using several methods and tools. The summary of the methods and tools used in the research are presented in the list below in a chronological order:

- Analysis of scientific literature and in-depth interviews for the formation of the hierarchic system of indicators
- Analysis of multi criteria decision making methods and selection of the suitable tool for quantitative evaluation of alternatives
- Development of the questionnaire and survey of experts on the importance of criteria (weights) and evaluation of each criteria by experts

The first step of the research was the analysis of the scientific literature on the topic of security in retail and related themes in order to gather background information on the topic of security in business and in retail in particular, identify the relevant criteria of assessment of the security in retail stores and prepare the basis for the interviews.

The next step in the research process was to conduct in-depth interviews. The interviews were conducted with one representative of “Brothers Engineering” and two representatives of “Group of companies Okhrana”. “Brothers Engineering” is a company that specializes in the maintenance of security systems and engineering systems for Russian enterprises. It is in the market for over 10 years. One of the core competences of the company is the organization of effective service specializing in the systems maintenance and technical support. The company focuses on the protection of the properties and minimization of the losses of the clients with the aim of creating safe and effective from the economic point of view environment for business development and competitiveness assurance. “Group of companies Okhrana” is one of the leaders of the market of comprehensive security systems and operates in this field for over 20 years. The company develops the technical security equipment sets, which is a set of interconnected technical and engineering tools that allows provision of security of the operations of the secured object, protection of the valuable items, property, information and health and

safety of the people and at the same time proving the information regarding the condition of the secured object to the personnel.

On the basis of the first and second stage of the research process, the hierarchic system of criteria was formulated and it is presented in Section 1.4. After the hierarchic system of indicators was formed, it was established that the problem is multi criteria in nature and requires a multi criteria decision making method for solving the problem. The next stage of the research process was analysis of multi criteria decision making methods. This stage is presented in Section 2.2. After researching the advantages and disadvantages of most commonly used multi criteria decision making methods, the suitable method was chosen in the end of section 2.2.

After the method of the analysis of the information was chosen to be APIS, the information that was required for the successful application of the method was collected, more precisely, the information on weight coefficients was required as well as the information on the value of the criteria. The information on weight coefficients was obtained through the survey of 12 experts from the companies mentioned above, “Group of Companies Okhrana” and “Brothers Engineering”. The questionnaire and the results of the survey are presented in the appendixes 1 and 2. Later, through sending the hierarchic system of criteria to experts, the evaluation of each criteria for each criteria was obtained for each of the case outlets.

After the criteria were evaluated by the experts, the framework for the security system assessment was formulated, developed and described in section 2.3. Framework application was described in section 3.1, following the steps of the developed framework. At that time, all the preparatory steps were already done and it was time to apply the APIS tool for the analysis of the information. The APIS tool was applied for the analysis of information gathered through interviews, survey, and evaluation. It was applied on the specific example of five case outlets and the precise application of the APIS tool can be seen in section 3.2. The last stage of research was results analysis.

Among the various methods used in this research, the key methods and tools were in-depth interviews, survey, and APIS software.

## **2.2. Methods for multi criteria selection of alternatives**

Security assessment is an MCDM problem, because it searches for solutions among conflicting criteria and indicators (Janeiro and Patel, 2015). The main goal in security evaluation is to identify and choose the most secured object among different alternatives. This process in general involves a large number of factors with multiple often conflicting dimensions. Facilitating and solving such difficult decision situation can become quite complex. Hence, a more formal and systematic approach to this type of problem may be necessary (Azapagic and Perdan, 2005). This leads us to a number of multi-criteria decision making or else called multi-

criteria decision analysis techniques. The appropriate MCDM technique will aid in problem analysis and resolution for a specific problem of security evaluation in retail.

Multi criteria decision making cannot be automated and it remains a task of a human, a manager. However, multi criteria decision making techniques were invented in order to provide guidance to the decision maker in finding out the preferred solution to the problem. Each of the presented multi criteria decision making techniques is created in order to make the process of decision making as efficient as possible (Stewart, 1992).

Decision-making in the context of security in retail is a complex process, often involving several groups of stakeholders, various decision criteria and several alternative solutions to the decision problem (Azapagic and Perdan, 2005). In the problem of security assessment in retail, the alternatives will be different retail objects, decision criteria will be various factors that put together lead to an increased level of security of such retail object and groups of stakeholders will include employees, management, customers and community. All these groups are interested in increased security in retail stores. The various alternatives, or retail objects, will be then compared against each other in order to produce a ranking of alternatives. This ranking of alternatives is produced by one of the MCDM methods in order to illustrate which retail object is the best one among the examples examined and then sort all the rest of retail objects according to their security level gauged by the experts and the technique used.

Azapagic and Perdan (2005) propose a framework which is based on multi-criteria decision analysis. This framework is presented in Figure 1 and it consists of the following three stages:

1. Problem structuring
2. Problem analysis
3. Problem resolution.

Problem structuring involves the identification and definition of the decision problem, identification of security issues and indicators, specification of alternatives and assessment of the preferences. Problem structuring was predominantly discussed in Chapter 1.

Problem analysis is the second stage of the proposed framework presented in Figure 2.1 and it follows the problem structuring stage. At this second stage, the following three steps should be undertaken, according to Azapagic and Perdan (2005):

- Preference modelling
- Comparison and assessment of alternatives
- Sensitivity, uncertainty and robustness analyses.

Preference modeling is a step when the guidance in identifying the preferred solution is provided through construction of a model of decision-makers' value system, including their

preferences into the equation. After the elicitation of preferences process, they are aggregated in order to allow the identification of the most acceptable alternative. There are a number of various MCDM methods and several classifications of these methods as well.

Most of these methods however are constructed in accordance to an intention of a decision-maker to make a choice that satisfies the preference the most in a logical and structured manner. One of the classifications of these methods categorizes the MCDM methods into two major groups:

1. Programming methods, including optimization methods, such as multi-objective optimization and satisficing methods, such as goal programming
2. Multi-criteria decision analysis, including elementary, value-based and outranking techniques (Azapagic and Perdan, 2005)

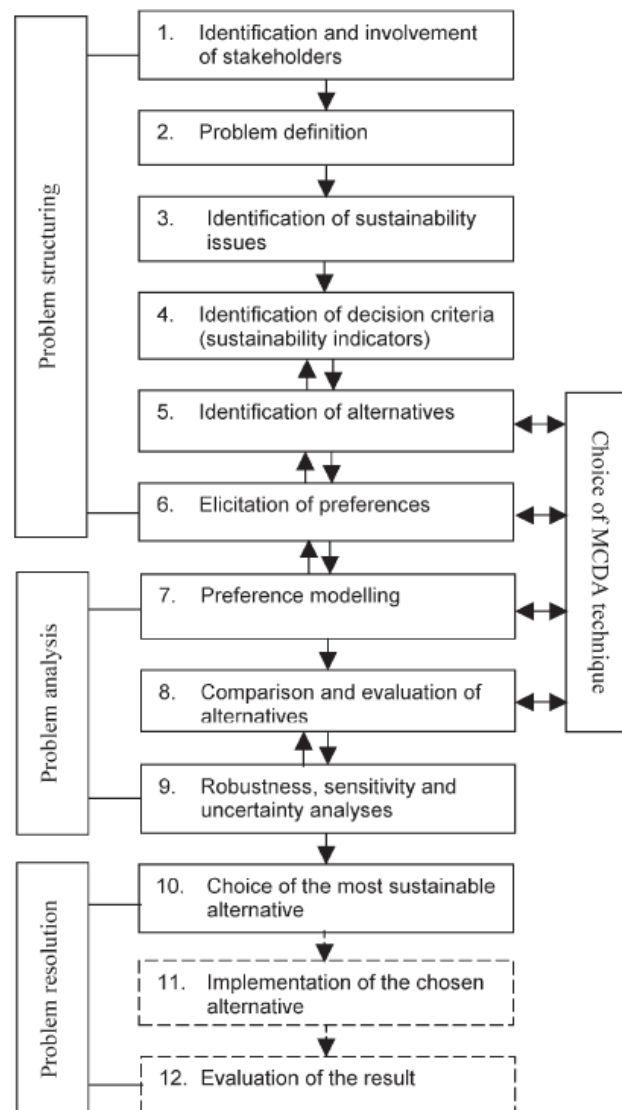


Figure 2.1. Integrated decision-support framework (Azapagic and Perdan, 2005)



The Table 2.1 presents a summarized overview of various existing MCDM methods.

Table 2.1. A summary of various MCDM methods (Adapted from Azapagic and Perdan, 2005)

Multi-objective optimization (Programming category)	Mathematical modelling is involved, simultaneously optimizes a number of criteria (Objectives), and has constraints. As a result it produces several Pareto optimal alternatives	Cardinal criteria
Goal programming (Programming category)	A decision-maker sets up goals for each criterion and then this method defines a preferred solution that has minimum deviations from the set goals	Cardinal criteria
Lexicographic method (MADA category)	First, the decision criteria are ranked according to importance. The preferred alternative is the one that scores best on the most important criteria.	Ordinal criteria Cardinal criteria Mixed criteria
Conjunctive method (MADA category)	Unacceptable alternatives are eliminated based on a minimum score for each criterion. Alternatives that do not meet acceptable levels for all criteria are eliminated.	Ordinal criteria Cardinal criteria Mixed criteria
Disjunctive method (MADA category)	Alternatives are considered valid if they meet the minimum level for at least one criteria	Ordinal criteria Cardinal criteria Mixed criteria
Maxmin/Maximax methods (MADA category)	Maxmin method differentiates among alternatives according to the criterion for which this alternatives shows worst results. The Maximax method has a reversed logic, comparing alternatives by the criteria they scored best in.	Ordinal criteria Cardinal criteria
Weighted sum	Overall performance of an alternative is calculated as a “weighted sum of evaluations for each criterion, and then used to make a choice.” (Azapagic and	Cardinal

	Perdan, 2005)a	
TOPSIS (Technique for order by similarity to ideal solution)	The preferred alternative is the one that is of closest distance to the ideal solution and farthest distance from anti-ideal solution. The ideal solution created through estimation of the best performance values for each criteria	Cardinal
MAVT (multi-attribute value theory)	Value function V is obtained through additive and multiplicative models, partial value functions are first determined and weights are established.	Cardinal
MAUT (Multi-attribute utility theory)	Utility function U is obtained through additive and multiplicative models, the function is obtained through first calculation of partial utility functions	Cardinal
AHP (Analytic hierarchy process)	Uses pairwise comparison matrices with eigenvalue method for recombination of the matrices into rating of alternatives	Cardinal
SMART (simple multi-attribute rating technique)	Uses weighted linear averages, they give close approximation of the utility functions. Ratio estimation is used for weight definition	Cardinal
UTA (Utility theory additive)	Uses ordinal regression for value estimations. Additive model is used in order to obtain the global value function.	Ordinal
EVAMIX	To indexes are calculated, one for cardinal and one for ordinal assessment. Then these two are combined to measure the supremacy among each pair of alternatives.	Ordinal Cardinal Mixed
ELECTRE family	There is a number of ELECTRE methods, all based on the outranking relationships.	Ordinal, Cardinal Mixed

There are a number of various decision-making methods that all attempt to solve a problem of chose among a distinct set of alternative decisions using numeric techniques. The earliest model proposed is weighted sum model (WSM). It is widely used in a variety of problems, however it has certain drawbacks to overcome which was presented a weighted product model (WPM). WPM can be thought of as a variation of the WSM. Later development of these methods is analytic hierarchy process (AHP), attributed to Saaty. Belton and Gear have created an alternative method, based on AHP, which is called the revised AHP. ELECTRE and TOPSIS methods are other methods that are widely used for similar problems of a given set of alternatives with weighted criteria for selection (Triantaphyllou, 2000). Russian professor Hovanov has developed an approach that is used for similar problems and is based on the special software APIS for the execution of the method. His method accounts for non-exact, non-numeric and non-??? Information on weights, which make this method especially applicable to the context of security evaluation problem, as it encompasses non-exact, non-numeric, and non-?? Information on weight coefficients.

All the methods mentioned above have the structure in common. Each of these methods uses numerical analysis of alternatives and thus has three steps in common:

1. First, the relevant alternatives and relevant criteria are determined
2. Second, the numerical measures are attached to the relative importance of the criteria as well as values of each criteria in relation to the alternative
3. In order to determine the ranking of each alternative, the numerical values are processed (Triantaphyllou, 2000).

Decision-making methods oftentimes lack the ability to exactly evaluate the applicable information. When the decision-making methods are applied to real life, the decision maker often encounters that information is inexact and fuzzy (Triantaphyllou and Lin, 1996).

### **The Weighted-Sum Model**

The WSM is perhaps the most widely used in practice for its relative simplicity of execution and ease of application. Let us examine the method based on maximization case, when the values of criteria are the higher the better.

Weight sum method is used frequently because of its relative ease of implementation. In the example illustrated in Table 2.2, a problem is characterized by  $m$  alternatives and  $n$  criteria, where  $m=3$  and  $n=4$ . Further, relative weights for criteria are given.

In this example, the problem is easily expressed in the matrix format. Every value in the table expresses the performance of a given alternative in terms of the corresponding decision criteria. The score for alternatives is calculated by using the following formula:

$$A_{WSM} = \max \sum_{j=1}^N q_{ij} w_j, \text{ for } i = 1, 2, 3, \dots, M.$$

and then depending on the initial problem type, whether it is maximization or minimization, either an alternative with a maximum value or with a minimum value is chosen. It is a standard method for Pareto set creation in multi-objective optimization problems. However, weighted sum method has two disadvantages (Das et al., 1997). First, with the even distribution of the weights on the objective function does not necessarily lead to an even distribution of solutions on Pareto front. Frequently solutions are seen in some parts of the Pareto front, while they are not seen in other parts of it. Second, this method does not find solutions on non-convex parts of the Pareto front, while such Pareto optimal solutions frequently exist (Kim et al., 2005).

Table 2.2. Example of the weighted sum method execution (Kim et al., 2005)

<i>Alternative<sub>i</sub> / Criteria<sub>j</sub></i>	Cr.1	Cr.2	Cr.3	Cr.4
Relative Weights ( $w_j$ )	0.15	0.40	0.25	0.20
Alt.1	35	30	25	40
Alt. 2	20	40	30	40
Alt. 3	40	20	40	20

The weighted-sum method can be easily applied in cases where all units of measurement are all the same (for instance, rubles, km, minutes, etc.). However there is an assumption embedded in the method, precisely, the additivity utility assumption and hence this method is not applicable to situations and problems including different units of measurement in them, because the conceptual violation occurs (Triantaphyllou and Lin, 1996).

### **The Weighted-Product Model**

“If weighted sum model used addition to rank alternatives”, “the weighted-product model uses multiplication”. The comparison of alternatives is done through multiplication of ratios for each criterion. All of these ratios are raised to the power of the comparable weight of the matching criterion. “In general, the following formula is being used for the comparison of the two alternatives  $A_K$  and  $A_L$ ”:

$$R\left(\frac{A_K}{A_L}\right) = \prod_{j=1}^N \left(\frac{a_{Kj}}{a_{Lj}}\right)^{w_j} \text{ (Triantaphyllou and Lin, 1996).}$$

Let us again consider the maximization case, that is, the higher the values, the better. In the maximization case, if the ratio above is greater or equal to one, then the decision maker can conclude that the alternative  $A_K$  is better than alternative  $A_L$ . Therefore, the alternative that needs to be chosen is that alternative that is better than all other alternatives or at least as good as all of

the other alternatives. The weighted-product method is very similar to the weighted sum method; it can be seen as a modification of the weighted-sum method. Another name for weighted-product method is “dimensionless analysis” because by its structure it eliminates any units of measurement. Hence, it overcomes the major weakness of the weighted-sum method and therefore can be used for both single and multidimensional decision-making problem. Additionally, the comparative values of measure of alternatives in matching to corresponding criterion can be replaced with actual values in weighted-product method (Triantaphyllou and Lin, 1996).

### **The Analytic Hierarchy Process**

In the AHP method, the final step is related to the construction of an  $M \times N$  matrix  $X$ . We would use the same notation and denote  $M$  as the number of alternatives (rows) and denote  $N$  as the number of criteria (columns). In this constructed matrix, the element  $a_{ij}$  represents the relative performance of the  $i^{th}$  alternative in terms of  $j^{th}$  criterion. The row vector  $X_i = (a_{j1}, a_{j2}, \dots, a_{jN})$  for the  $i^{th}$  alternative ( $i=1,2,\dots, M$ ) is actually the eigenvector of an  $N \times N$  reciprocal matrix, determined through a series of pairwise comparisons. For each of these vectors, the elements add up to one. The AHP does not use the actual values, but rather uses the relative ones instead. As weighted-product model it can be used in both single and multidimensional decision problems. The formula used by the AHP is actually the same one as the formula used by weighted-sum model (Triantaphyllou and Lin, 1996).

### **The Revised Analytic Hierarchy Process**

Belton and Gear (1983) proposed this method, later it was accepted by the originator of AHP method, Saaty and now is also known by the name ideal-mode AHP. This method was derived out of observation that Belton and Gear noticed. They noticed that in some cases AHP yields unjustifiable ranking reversals. For instance, in the example that they give they introduce a new alternative which is identical to a non-optimal one. As a result of this new alternative introduction, the ranking results for the existing alternatives change. Belton and Gear proposed that the reason for this ranking inconsistency lies in that all the comparative performance measures of alternatives for each criterion is summed to one. Instead, they argue that the relative value of each alternative will be divided by the maximum value in the matching vector of comparative values.

### **The TOPSIS Method (Technique for order preference by similarity to ideal solution)**

This method was developed by Hwang and Yoon (1981) with the aim of providing an alternative method to the existing ELECTRE method. TOPSIS assumes that the distance

between the alternative that is need to be chosen and the ideal solution should be the shortest while the distance between the alternative that is need to be chosen and the anti-ideal solution should be the farthest in a geometrical sense. TOPSIS evaluates a decision matrix through a series of steps, which are an adaptation from the ELECTRE method.

1. Normalized decision matrix construction
2. Weighen normalized decision matrix construction
3. Ideal and anti-ideal solutions determination
4. Separation distance calculation
5. Comparative closeness to ideal solution calculation
6. Ranking of the alternatives

### **Methods in use**

For the creation of the security rating index for industrial construction projects Sylvie et al. (2013) used Analytical Hierarchy Process method for weights coefficients determination. Security rating index was developed in order to quantitatively evaluate the level of security for a given project. According to the authors, security rating index would provide increased utility because the degree of use of each security practice will be scored. This, according to the authors will significantly increase the value of previously used checklist of security practices and create additional value. The security rating index constructed by the authors is limited by the scope of it. The security rating index is developed for the heavy industrial sector (Sylvie et al., 2013). It will be interesting to see how similar approach can be used for the construction of security index for retail industry. Sylvie et al (2013) states that the approach used in the research allow to compare projects with similar security considerations. Security rating index is called a tool for integration of risk, impact, and security best practices. It is created to aid companies in assessing the level of security against similar projects. Additionally, the authors state that after a number of tests certain norms could be established for projects with similar threat and impact levels across all projects in the industry. Moreover, authors state that this security rating index could be used for a more cost-effective security considerations integration in the projects.

Borisenko (2013) lists several methods for weights coefficients determination: the direct quantitative evaluation of coefficients, ranking of factors, method of pairwise comparison, analytical hierarchy process. The author also states that the above-mentioned methods are applicable to diverse systems of quality evaluation that deal with the processes and events in different enterprises.

Andre et al. (2009) uses multi-criteria analysis for the evaluation of management system. The management system is a complex system. It consists of different elements, each of which has its own functions within the system. Andre et al. (2009) states that multi-criteria analysis is

among the most reliable methods for conducting an evaluation of the system's property such as quality or sustainability.

In the paper, the author states that complexity is a property characterized by the diversity of elements with defined functions. Additionally, the state of complex system can be described by complexity. The author cites examples of complex system as well. The authors' examples include a DNK molecule from biology, or internet network from information theory. For these systems, the complexity is expressed as wholeness. Therefore, complexity is the essential characteristic of the system. For instance, for the internet system, the increase in transfer of information will be equivalent to the increase in complexity of the system. Therefore, the main property of the system is its complexity and it can be substituted with the major characteristic of the system.

In the analysis, the authors used a system of indicators, which are major parameters of the system. The indicators were of different scales and were therefore converted to be expressed in the same scale. Then, the convolution of the indicators resulted in the integral measuring parameter which reflects the total quality of the system. The author calls it multi-criteria General Management Index and uses it for the evaluation of the quality of the management system. The author also states that the improvement of the system will result in increase of the General Management Index (Andre et al., 2009).

### **APIS method**

The decision support system APIS is created for holistic evaluation of specific systems in the environment of uncertainty of the complex multi-parametric objects. Objects of the evaluation may be complex technical systems, various managerial and organizational issues, expert opinions, economic objects such as stores, banks, insurance companies and so on. The properties of evaluation could be effectiveness, efficiency, reliability, applicability, security, profitability, and so on. DSS APIS is a universal tool applicable in circumstances of non-numeric, non-exact and deficient information (Hovanov et al., 2009). Among various problems that could be solved with the use of DSS APIS, the most common are:

- Support of decision-making process in situations characterized by prevalence of qualitative information that cannot be directly described numerically
- Evaluation in the environment of uncertainty of effectiveness, quality or other property of a complex system of various implications and its projects
- Multi-criteria selection of the course of action given the uncertainty of the importance of individual criteria and support in the identification of the preference of the decision-maker

- Synthesis of the collective opinion of a group of experts in the environment of information deficiency of the degree of reliability of a single expert
- Creation of a hierarchical system of evaluation of complex multi-level objects or properties given the information deficiency at each level of hierarchy

The essence of the DSS APIS is the method of aggregated indicators, which is the convolution of multiple characteristics of the complex object or property into the aggregated index, which represents a convoluted (aggregated, integral, general, etc. ) indicator, synthesizing individual indexes that characterize the property of an object, such as effectiveness, reliability, security, profitability and so on (Hovanov et al, 2009). An object in the analysis should be a complex multi-criteria system, such as an alternative course of action, a good or service, a store, bank or an insurance company, and so on.

The method behind the DSS APIS is as follows:

1. Individual characteristics vectors formation
2. Selection of the aggregation function
3. Determination of the vector of weight coefficients

The third step is the most interesting step in the procedure that DSS APIS performs. Actually, the researcher is rarely given the exact weight-coefficient of the variety of characteristics. In general, the researcher possesses only non-numeric, non-exact and deficient information on weight-coefficients. Sometimes, however, the researcher has interval information on relative importance of characteristics and therefore relative importance of weight-coefficients, which may be expressed as an inequality, such as  $w_1 > w_2 > w_3$  (Hovanov et al, 2009).

APIS was chosen as a tool for information analysis because it has uniquely combines several characteristics and other methods examined do not possess the same set of characteristics as APIS. It is the combination of all the APIS characteristics that makes it such a valuable tool, because the characteristics by themselves may characterize other methods as well, however only APIS uniquely combines all of them. These characteristics are:

- It is applicable in the condition of uncertainty
- It allows to analyze a hierarchic system of criteria
- It has a complementary software for precise and accurate calculations
- It gives out the range of the convoluted index, therefore allowing to get an understanding of the risks related to the certain value
- It allows to work with inexact information (Hovanov et al, 2009).



### 2.3. Framework of security system assessment

The developed framework of security system assessment is a series of stages, presented in Figure 1. The consecutive execution of the six stages allows performing a comprehensive assessment of the store security system, identifying weak elements of the security system and formulating recommendations on the ways to improve the security level in the store.

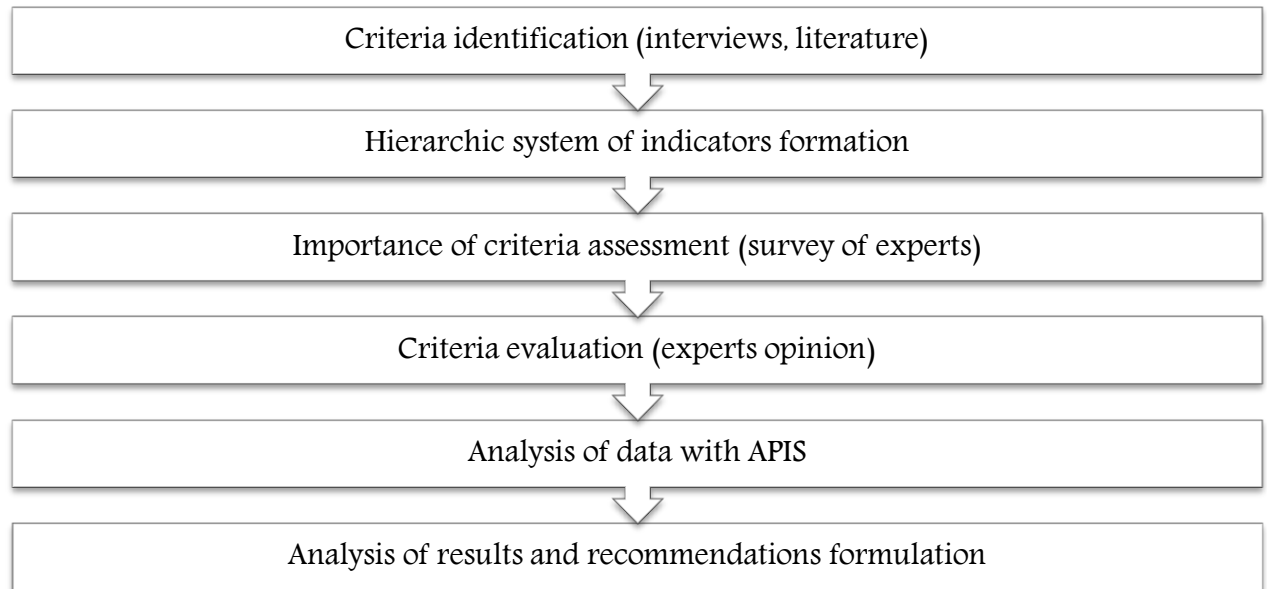


Figure 2.2 Framework of security system assessment (Author, 2017)

The first stage of the framework is criteria identification. It is done through both literature research and interviews. At first, the background information on the security system assessment of a particular business entity, common practices, and the most common countermeasures used are analyzed in order to have a general understanding of the problem. Most likely, several criteria will be identified at this stage, although typically it will be the criteria of the first or second level of the hierarchic system of indicators, formed later. After the preliminary research of scientific literature is done, the top level of the hierarchic system of indicators is usually identified. The next step is to confirm the criteria developed through literature research through the in-depth interviews with experts. The selection of experts for the interview is very important at this stage. The person who is being interviewed should be knowledgeable about security systems, common practices of this type of business entity (for instance for the purposes of this thesis the person who is being interviewed was knowledgeable about the common practices in the retail industry related to security, while if other type of business entity is analyzed, the interviewee should know about the practices of that particular business entity type).

The second step is the formation of the hierarchic system of indicators. During the first stage of criteria identification it was noted that each criteria has sub criteria and overall the

structure of the list of criteria reminds a hierarchy. Therefore it was decided to organize the identified criteria in a hierarchic system.

Since the method of data analysis was already chosen to be APIS, the next stages of the framework reflect the specifics related to APIS, more specifically the next stages prepare the data in such format that will be convenient to analyze with APIS. The third stage of the framework, the importance of criteria assessment helps to identify the weight coefficients and make the analysis more precise. Even though it is possible to analyze the hierarchic system of indicators without the exact weights using APIS tool, knowing the coefficients increases the accuracy of the calculations and makes the overall end result more precise, making this stage an important one. The importance of criteria assessment is done through the survey of experts. In this case, the questionnaire was developed based on the previous research, in particular the publically available master theses that used APIS for the analysis of data as well were examined and on the basis of the previously published works the questionnaire was developed. The questionnaire gradually covers all the levels of the hierarchic system of indicators, asking to assess the relative importance of the criteria. The relative importance is then analyzed and based on the results the weight coefficients are determined with the use of APIS. APIS only allows to define comparative relationships for each criteria, and is not designed to insert the precise weight coefficients.

During the next stage, the criteria are evaluated by the experts. At this stage, the expert who analyzes and evaluates the business entities (in this case, grocery retail stores), must be knowledgeable about the businesses he or she analyzes, have an expertise in the field of security and ability to assign relative values for each of the criteria. For instance, enough information should be available to the expert to say for example whether the EAS or the specific management practice at one business entity is better or worse than at another store, as well as by how much they differ. Careful selection of experts for this stage is also very important.

The next stage is the analysis of the data with APIS. To illustrate how this is done, let's consider an example. Let's assume that there are three retail stores that will be analyzed according to four criteria. Supposedly the criteria are evaluated as presented in Table 2.3.

After this is done, the next step is to allocate weights to each criteria. In this example, the following relationships were set:

- Assessment Criteria 1 > Assessment Criteria 2
- Assessment Criteria 2 > Assessment Criteria 3

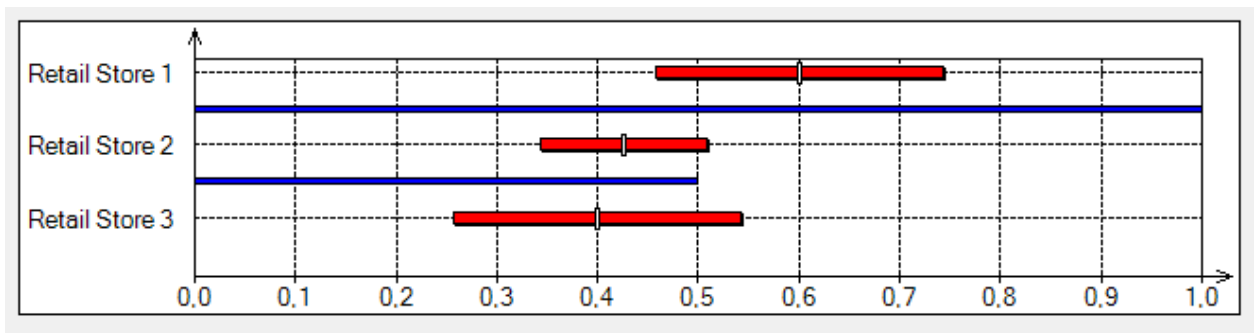
After the relationship for weight coefficients are set, the next step is to run calculations in APIS software. This gives out a ranking of alternatives, in our case retail stores, in order of their

security level. The example of how the ranking looks like for the given retail stores is presented in Figure 2.3.

Table 2.3. Evaluated assessment criteria example

	Assessment Criteria 1	Assessment Criteria 2	Assessment Criteria 3	Assessment Criteria 4
Retail Store 1	7	5	5	4
Retail Store 2	6	6	7	4
Retail Store 3	5	7	6	7

Figure 2.3. APIS calculation result example



In this example with three retail stores, we could see that the retail store 1 has the best security level, followed by retail store 2 and retail store 3. APIS gives out the range into which the exact value of the index will fall, and although the ranking shows that retail store 1 is better than retail store 3 in terms of security, it also shows that the values of the two overlap, meaning that their order in the ranking in terms of security level may be as well reversed.

The last stage of the framework is the analysis of results and recommendation formulation; this is specifically illustrated in chapter 3. In chapter 3, a specific example of 5 grocery retail stores is taken and analyzed, and at the end of it the recommendations for each store are presented. Coming back to the example that we used to describe the procedure of analysis of information in the APIS, the stage of recommendation formulation can also be illustrated on this example. For instance, if we see that retail store 3 takes the last place and has the lowest level of security in our example, we could then see what exactly resulted in such low security. Looking at the evaluated criteria table, it can be concluded that retail store 3 has to focus on assessment criteria 1 and 3 for the improvement of the current level of security. Therefore, analysis of the results not only gives us a comparative distribution of the stores in

order of their security level, but also allows identification of the exact reasons causing the lower level of security than desired.

Although the framework was primarily designed for application on retail stores, it is possible that the framework is also applicable in a different context, because the framework is a method of analysis first of all and if the interviews are conducted for a different type of a business entity and the experts will be carefully selected for the evaluation of the criteria importance and criteria values, then the similar series of stages will be also applicable to a non-retail context.

The framework was designed for the application in the retail context, and later applied on the grocery retail stores. Using the same criteria that were identified during the interviews the framework can be applied in the context of non-grocery retail as well, such as clothing stores or department stores. If the researcher who is willing to conduct a security system assessment of the business entity would follow the framework steps from the beginning and develop a different set of criteria rather than presented in this work, then the framework will be applicable in a non-retail context as well.

## **CHAPTER 3. APPLICATION OF THE FRAMEWORK TO THE CASE OUTLETS**

### **3.1. Retail business and case companies description**

A 2016 retail consumer research by Accenture on retail industry reports that 71% of retailers have loyalty programs, 10% try to collect name, address, e-mail and phone number information in the store while 57% of shoppers are concerned whether their favorite retailer is safeguarding their personal information. This brings us back to the first chapter, where we talked about the importance of information security nowadays.

The Accenture report also states, that smartphone usage to find the needed item is growing in popularity. Also, 39% of global retailers surveyed have smartphone apps with purchase capabilities, however only 31% of shoppers surveyed find it simple to purchase via mobile devices. A report by PwC also confirms these findings about the growing usage of mobile devices in the process of making purchases. Along with that, social media plays a significant role in customers' shopping experience, because customers rely on it as well as on the opinion of people in their network, advertising messages, and media coverage when they are making product decisions or choose among a variety of brands. However, 55% of purchases happen in the physical store globally.

In Europe, shoppers said that the following features would be nice to have for a grocery retail store:

1. The opportunity to check the product availability online before actually going to the store
2. The ability to order out of stock items in stores easily

However none of the stores that were evaluated in the research provide store-specific stock availability information. And only 6% have specific store staff who is able to order out of stock items for shoppers and 6% have in-store kiosks for ordering out of stock items. European stores have next day delivery options in 61% of the cases and 11% have same day delivery options.

Retail industry is the end point of the supply chain, where goods are purchased by the end consumer. A developed network of retail stores in the infrastructure by its presence is capable of demand stimulation, because it can increase the number of contacts between the goods on shelves and the potential consumer. Having a developed network of retail stores can also be a stimuli for supply increase, because in case of a developed network of retail stores customers save their time that would be otherwise spent on getting to the store or wasted in lines (Butov,2016).

Social importance of grocery retail is immense, since the majority of the population visit grocery stores at least twice a week. This frequency of consumer visits to a store can be explained by two factors: first, there is a need of daily food consumption; second, the goods that are consumed daily, such as poultry and milk are perishable and hence must be replaced frequently. Stable supply of food items is important in for a political stability as well. Inconsistency in food supply may provoke riots in the population. From the point of view of a modern government, a well-developed infrastructure of grocery retail stores is important for stable functioning of the state (Butov, 2016).

Russian economy development is characterized by privatization that occurred in the 90-s of the last century. So companies that participate in retail trade of grocery goods in the majority operate as companies with private property. A distinct trend nowadays is consolidation into several market leaders. This process develops as a creation and expansion of chain retail stored. This tendency allows realizing the economy of scale associated with the decreased marginal costs of enterprises. On the other hand, the consolidation leads to increased influence of the top market players, which in turn leads to these top players pressuring the market, including both suppliers and consumers (Butov, 2016).

The industry is also important because it involves a large part of the population in its operations. Grocery retail trade is a segment that is typically populated by small enterprises. However the current conditions are not that attractive. Other industries that are related to grocery retailing are construction market and rental market of commercial property. Grocery retailing serves as a driver of these markets by formulating the level of demand (Butov, 2016).

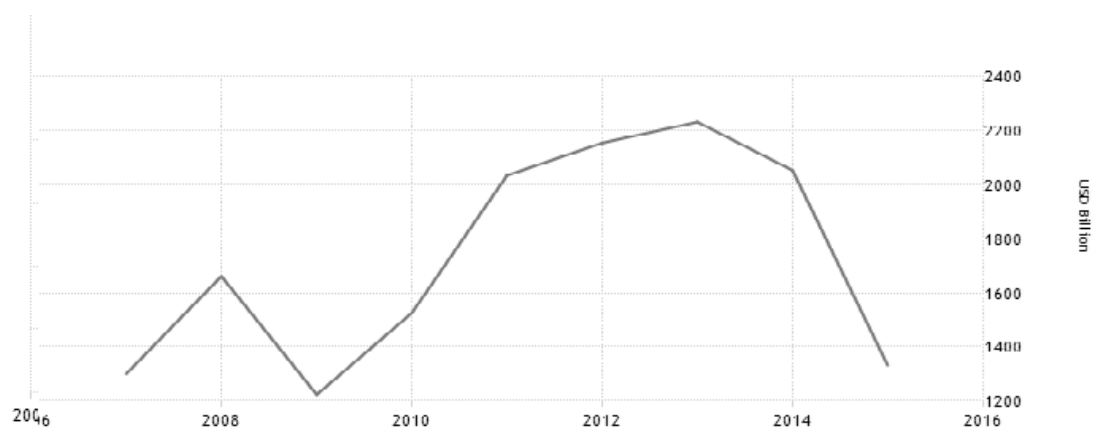


Figure 3.1. Russian GDP for the years 2006-2016 (Trading Economics, 2017)

Economic crisis inevitably has its impact on the state of grocery retail trade. Due to the crisis that hit the world economy and then Russian economy as well, the graph in figure 3.1 shows downward trend in the year 2009. Starting the year 2010, the retail market began to show upward dynamic, however later on the trend went down again. Currently the market is regaining the position it had in 2010. Key drivers of retail industry are consumer demand and high oil

prices in Russia. Retail is one of the key indicators of overall economy and it mimics or at least reflects the GDP trends. Russian GDP for the years 2006-2016 is presented in Figure 2 (Ishenko, 2016).

Major changes can be seen in the price sensitivity of consumers. Overall meat consumption is decreasing, however it seems like beef is being substituted by poultry and pork consumption. Even though the economy is plummeting, because the grocery products are essential commodities, there will not be a drastic drop in consumption. Moreover, experts note that a consumer has a tendency to consume more food during crisis in compensation of saving on trips or luxury goods consumption (Butov, 2016).

Figure 3.2 shows the distribution of market share among top retailers. “Magnit” is number one by markets share in the list. “X5 Retail Group” and “Auchan” follow with the second and third place respectively. Retail chains “Dixi” and “Lenta” follow with the fourth and fifth places (Ischenko, 2015).

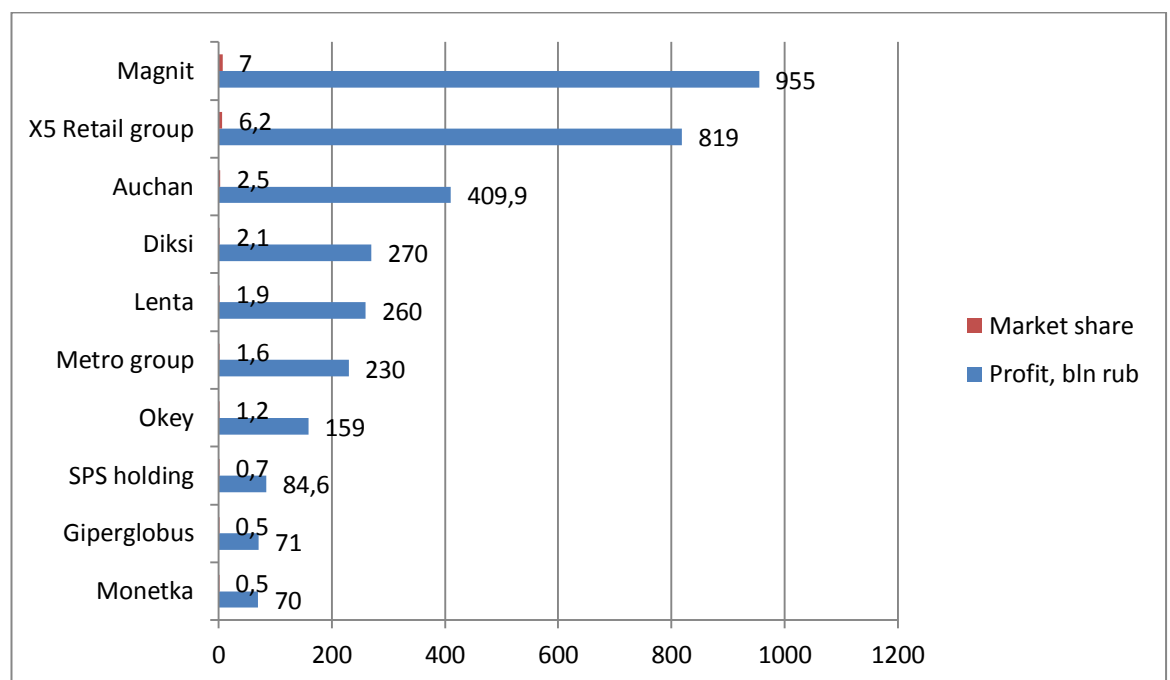


Figure 3.2 Top Russian retailers market share for the year 2015 (Ischenko, 2015)

Figure 4 shows the distribution of market shares among major retail formats for the year 2015. Markets take up 7%, followed by modern non-chain retail stores (16.5%). Next segment is taken by top-7 retailers and other retail chains. Traditional stores segment is the largest.

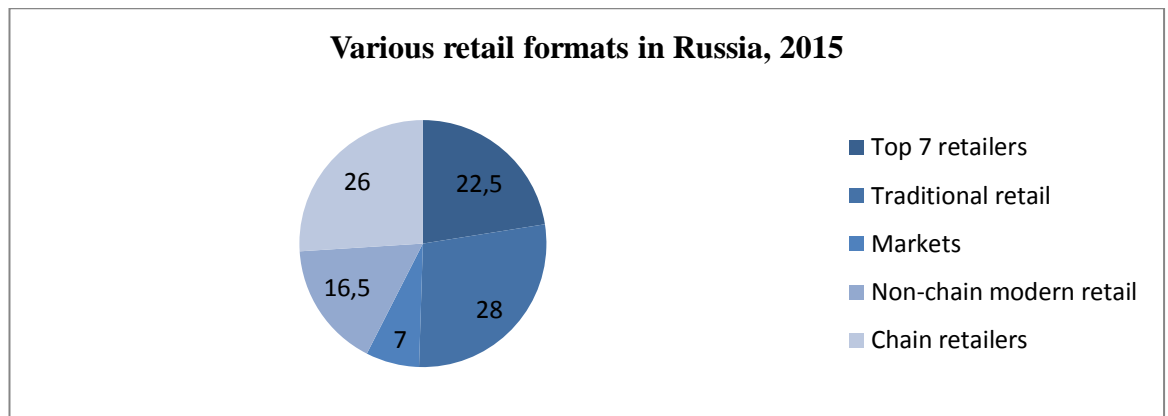


Figure 3.3. Various retail formats and their share in the Russian market (Ishenko, 2015)

Household consumption decreased over the past couple years, and it is expected that income will continue to decrease during the next year. Consequently, consumers currently tend to be more price-cautious and choose close to home alternative retailers. Even though overall retail market experiences the diminished customer demand and decreased profits, the segment of close to home grocery retails shows positive dynamics (Ishenko, 2015).

### 3.2. Framework application

The framework is presented in section 2.3. The graphical representation of the framework can be seen in Figure 2.2. To this point in the thesis, the first stages of the framework were already described. The analysis of scientific literature as well as the results from the in-depth interviews was presented in the first chapter. The hierarchic system of indicators illustrating the relevant criteria was formed and presented in section 1.4.

The next stage is the assessment of the importance of the criteria. As described in the methodology section of this thesis, the assessment of the importance of criteria was done through the survey of experts. The Questionnaire for the survey as well as the results of the Questionnaire are presented in Appendices 1 and 2. Appendix 1 presents values that the researcher has received through survey of 12 experts in the field of security. It presents relative importance of each criteria estimated by each of the respondents as well as the average value of importance for each of the criteria. The next stage is evaluation of criteria by experts, the results of this evaluation are presented in Table 3.1.

The aggregated preference indices calculation was done in several steps:

First, the aggregated preference indices were calculated for internal theft protection, then for external theft protection, supplier fraud protection, administrative error protection, and lastly for the cyber threat protection. Each of these five groups of characteristics had two sub-sections: organizational countermeasures and technical countermeasures.

The values used in the calculations were obtained through interviews with experts in security field and are presented in the table 3.1.



Table 3.1. Criteria values (Author, 2017)

	Pyaterochka	Magnit	Diksi	Ideya	811
<b>Internal Theft Protection</b>					
<i>Organizational Measures</i>					
Rewards system	2	5	2	1	3
Pre-employment screening	2	4	4	2	4
Awareness programs	1	3	3	2	5
Internal audits	2	2	3	2	6
Mystery shopping	2	1	2	1	1
Security team work	2	5	2	2	6
Customers involvement	1	2	1	1	1
Employees education	2	4	4	2	5
Polygraph control	1	1	6	1	1
Collective liability	2	1	2	2	1
<i>Technical Measures</i>					
Cashier control system	2	1	1	1	6
Labor hours control system	1	1	2	1	1
Access control system	4	4	4	3	3
CCTV system	6	3	2	5	5
Burglar alarm system	3	2	3	2	3
Mirrors	1	1	2	2	1
<b>External Theft Protection</b>					
<i>Organizational measures</i>					
Customer awareness programs	3	2	4	3	2
Loss prevention specialist	2	3	2	4	1
Security guard	4	3	4	2	4
Rapid response team	3	2	3	2	3
Lawsuits handling	1	2	3	1	2
<i>Technical measures</i>					
EAS					
Passage width	4	4	5	4	1
Tag detection probability	2	5	5	3	1
Forced activation possibility	1	2	1	2	1
CCTV					
Cameras resolution	6	5	2	5	4
Archive depth	4	5	3	4	4
Movement detection	7	6	7	5	7
Pre-alarm function	7	6	6	7	5
Degree of integration	2	1	2	2	1
Face recognition	1	1	2	3	2
Burglar alarm	5	5	4	5	4
Mirrors	3	4	2	5	4
<b>Supplier Fraud Protection</b>					
<i>Organizational measures</i>					
Goods receipt regulations	4	6	5	3	5
<i>Technical measures</i>					
CCTV	6	6	2	2	4
Goods receipt control	1	2	1	1	2
Barcodes scanners	7	7	7	7	1

Video-logistics systems	1	1	5	1	1
Sealing and transportation rules	5	5	5	3	3
<b>Administrative Errors Protection</b>					
<i>Organizational measures</i>					
Documentation regulations	3	4	4	3	2
ABC analysis	2	3	3	2	4
Conversion	1	2	1	1	3
<i>Technical measures</i>					
System of document flow	3	4	3	2	2
Automated controls	4	2	3	3	2
CCTV	6	6	2	2	4
Lines control system	1	1	2	1	1
Regulations control	4	6	4	2	5
Customers count	2	2	1	1	1
Face recognition system	1	2	1	1	2
<b>Cyber threats protection</b>					
<i>Organizational measures</i>					
Vulnerability tests	1	2	1	1	2
Employees training	2	3	2	1	1
Management	2	2	2	1	1
<i>Technical measures</i>					
Protection mechanisms	2	2	2	1	1

At the first step the internal theft protection characteristic was evaluated, including all the relative weights information gathered by the survey. The following relationships were set:

- $w(\text{Rewards system}) < w(\text{Internal audits})$
- $w(\text{Polygraph control}) > w(\text{Internal audits})$
- $w(\text{Pre-employment screening}) = w(\text{Collective liability})$
- $w(\text{Mystery shopping}) = w(\text{Reward system}) = w(\text{Customer involvement})$
- $w(\text{Internal audits}) = w(\text{Employees education})$
- $w(\text{Security team work}) = w(\text{Polygraph Control})$
- $w(\text{Mystery shopping}) < w(\text{Internal audits}) < w(\text{Security team work})$

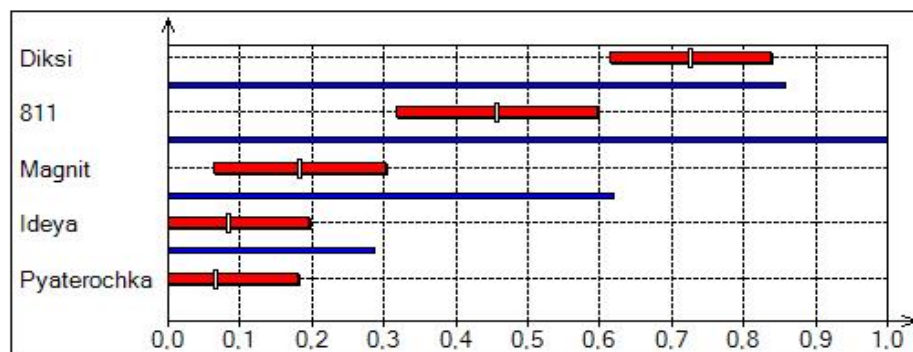


Figure 3.3. APIS output for internal theft protection: organizational measures

After the information on relative weight of criteria was input, the APIS software calculated the following aggregated preference indices for internal theft protection, presented in Figure 3.3.

	Pyaterochka	Magnit	Diksi	Ideya	811
Index	0.0667	0.1817	<b>0.7270</b>	0.0833	0.4571
Rank	5	3	1	4	2
St Dev	0.1127	0.1191	0.1106	0.1106	0.1400

Table 3.2. Aggregated preference indices for Internal Theft Protection: Organizational measures characteristic

Table 3.2 states the exact values of the indexes that were calculated for each store. As we could see by looking at Figure 3.3, “Diksi” has scored the highest in the internal theft protection criteria, followed by “811” and “Magnit”, while “Ideya” and “Pyaterochka” finished the list with lower indices. Additional output includes the weight-coefficients estimations visualization and statistics of admissible weight-coefficient values, presented below in Figures 3.4 and Figure 3.5.

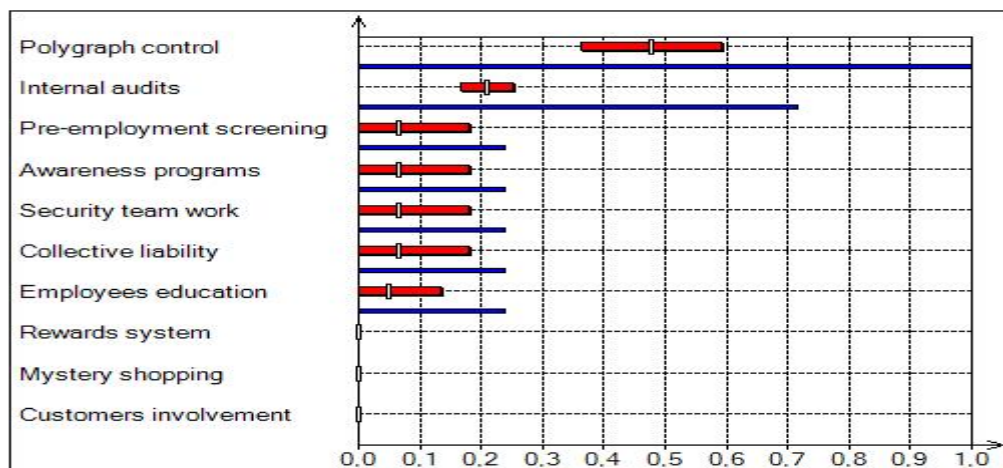


Figure 3.4. Weight-coefficients estimations visualization for Internal Theft Protection: Organizational Measures characteristic

Weight of index	Min	Max	Mean	StDev	Rank
w(Rewards system)	0,0000	0,0000	0,0000	0,0000	5
w(Pre-employment screening)	0,0000	0,4000	0,0667	0,1127	3
w(Awareness programs)	0,0000	0,4000	0,0667	0,1127	3
w(Internal audits)	0,2000	0,4000	0,2095	0,0426	2
w(Mystery shopping)	0,0000	0,0000	0,0000	0,0000	5
w(Security team work)	0,0000	0,4000	0,0667	0,1127	3
w(Customers involvement)	0,0000	0,0000	0,0000	0,0000	5
w(Employees education)	0,0000	0,2000	0,0476	0,0852	4
w(Polygraph control)	0,4000	0,8000	0,4762	0,1151	1
w(Collective liability)	0,0000	0,4000	0,0667	0,1127	3

Figure 3.5. Statistics of admissible weight-coefficients values

The APIS output for the further steps will be presented in the Appendix 3. Only the tables with the exact values of the indexes will be shown in the body of the thesis.

The next step was to calculate the indices for “Internal Theft Protection: Technical measures” characteristic. This was done using the information gathered in the survey on the relative importance on criteria. The following rules were set:

- $w(\text{Cashier control system}) > w(\text{Labor hours control system})$
- $w(\text{Labor hours control system}) > w(\text{Access control system})$
- $w(\text{CCTV system}) > w(\text{Mirrors})$

In the Appendix 3, Figure 1 we could see the ranking of our alternatives, it looks like the “811” store is ranked number one, followed by Pyaterochka, Diksi, Ideya, and Magnit. The Table 3.3 shows the rank of each of the stores, standard deviation and index of each.

	Pyaterochka	Magnit	Diksi	Ideya	811
Index	0.427	0.067	0.267	0.200	<b>0.733</b>
Rank	2	5	3	4	1
St Dev	0.075	0.024	0.094	0.071	0.024

Table 3.3. Aggregated preference indices for Internal Theft Protection: Technical measures

The third group of characteristics that was examined was “external theft protection: organizational measures”. The results obtained through running the calculations in APIS software are presented in Table 3.4. The more detailed information with additional output from APIS is presented in the Appendix 3 in Figures 4, 5, and 6.

	Pyaterochka	Magnit	Diksi	Ideya	811
Index	0.572	0.411	<b>0.622</b>	0.583	0.383
Rank	3	4	1	2	5
St Dev	0.183	0.174	0.179	0.261	0.261

Table 3.4. Aggregated preference indices for “external theft protection: organizational measures”.

Next, on level lower, the EAS system characteristic was evaluated. The following formation rules were set:

- $w(\text{tag detection probability}) > w(\text{forced activation possibility})$
- $w(\text{passage width}) < w(\text{forced activation possibility})$

	Pyaterochka	Magnit	Diksi	Ideya	811
Index	0.233	<b>0.972</b>	0.711	0.672	0.000
Rank	4	1	2	3	5
St Dev	0.118	0.034	0.269	0.120	0.000

Table 3.5. Aggregated preference indices for EAS

Table 3.5 presents the aggregated preference indices for the EAS system, identifying the store with the best EAS system and all the following stores in the order. The visualization of this ranking as well as the information on weight coefficients are presented in the Appendix 3 in Figures 7, 8, and 9.

Next, the procedure was repeated for CCTV. The following rules were set:

- $w(\text{cameras resolution}) > w(\text{degree of integration})$
- $w(\text{face recognition}) = w(\text{degree of integration})$
- $w(\text{archive depth}) < w(\text{face recognition})$

	Pyaterochka	Magnit	Diksi	Ideya	811
Index	<b>0.783</b>	0.455	0.400	0.738	0.467
Rank	1	4	5	2	3
St Dev	0.211	0.199	0.238	0.197	0.170

Table 3.6. Aggregated preference indices for CCTV

Next, the whole characteristic of external theft protection: technical measures was evaluated. The following rules were set:

- $w(\text{EAS}) < w(\text{CCTV})$
- $w(\text{EAS}) = w(\text{Burglar alarm})$
- $w(\text{Mirrors}) < w(\text{EAS})$

	Pyaterochka	Magnit	Diksi	Ideya	811
Index	0.810	0.486	0.183	<b>0.852</b>	0.105
Rank	2	3	4	1	5
St Dev	0.066	0.121	0.063	0.031	0.025

Table 3.7. Aggregated preference indices: external theft protection: technical measures

Table 3.7 shows the output indexes for each store for the technical measures of external theft protection. The additional output from APIS is presented in Appendix 3, Figures 13, 14, and 15.

Next, the supplier fraud protection: technical measures characteristic was evaluated using the following set or rules:

- $w(\text{barcodes scanners}) < w(\text{CCTV})$
- $w(\text{goods receipt control}) = w(\text{video-logistics systems})$

Table 3.8 shows the index values for each store on the criteria of supplier fraud protection: technical measures.

	Pyaterochka	Magnit	Diksi	Ideya	811
Index	0.652	<b>0.826</b>	0.400	0.052	0.387
Rank	2	1	3	5	4
St Dev	0.252	0.207	0.232	0.097	0.194

Table 3.8. Aggregated preference indices: supplier fraud protection: technical measures

The additional output from APIS related to the criteria of supplier fraud protection, technical measures is presented in the Appendix 3 in Figures 16, 17, and 18.

Next, the administrative error protection: organizational measures characteristic was evaluated, all criteria were estimated to be of the same importance so in this case we got same weight-coefficients for all three of the criteria.

	Pyaterochka	Magnit	Diksi	Ideya	811
Index	0.167	<b>0.667</b>	0.500	0.167	<b>0.667</b>
Rank	3	1	2	3	1
St Dev	0.149	0.149	0.258	0.149	0.298

Table 3.9. Aggregated preference indices: administrative error protection: organizational measures

We could see from Table 3.9 that in this case we have received two sets of equal values. Magnit and 811 are ranked “1” and Pyaterochka and Ideya also share a rank of “3”.

We could see from the figure 20 in the Appendix 3 that weight coefficients are of the same values, equally sharing the importance which corresponds to our answers received for survey where the respondents have on average assigned equal importance to these characteristics.

Next, administrative errors protection: technical measures characteristics were evaluated with the series of rules set:

- $w(\text{CCTV}) < w(\text{customers count})$
- $w(\text{customers count}) < w(\text{lines control system})$
- $w(\text{regulations control}) > w(\text{system of document flow})$

	Pyaterochka	Magnit	Diksi	Ideya	811
Index	0.325	0.500	<b>0.625</b>	0.000	0.238
Rank	3	2	1	5	4
St Dev	0.043	0.100	0.083	0.000	0.089

Table 3.10. Aggregated preference indices: administrative errors protection: technical measures

The results obtained are shown in table 3.10 and in the Appendix 3 in Figures 22, 23 and 24. Next, cyber threat protection: organizational measures characteristic was evaluated, given the following rules for weight coefficients:

- $w(\text{vulnerability tests}) > w(\text{employees training})$
- $w(\text{employees training}) = w(\text{management})$

	Pyaterochka	Magnit	Diksi	Ideya	811
Index	0.344	<b>1.000</b>	0.344	0.000	0.600
Rank	3	1	3	4	2
St Dev	0.241	0.000	0.241	0.000	0.600

Table 3.11. Aggregated preference indices: cyber threat protection: organizational measures

**Next stage** was to move to the level 3 of hierarchy and compute the aggregated indexes for five characteristics: internal theft protection, external theft protection, supplier fraud protection, administrative error protection, and cyber threat protection.

First, the aggregated indexes for internal theft protection are computed with the following criteria on the weight-coefficients:

- $w(\text{organizational measures (ITP)}) > w(\text{technical measures (ITP)})$

These results from the survey make sense because for the prevention of the internal theft organizational measures are indeed more important, this was discussed in the first chapter as well.

	Pyaterochka	Magnit	Diksi	Ideya	811
Index	0.108	0.139	<b>0.860</b>	0.059	0.673
Rank	4	3	1	5	2
St Dev	0.088	0.028	0.114	0.029	0.067

Table 3.12 Aggregated preference indices: Internal Theft Protection

In terms of internal theft protection characteristic, we could see that Diksi and 811 seem to be far better off in this rather than the rest of the stores. Diksi and 811 are much differentiated from the rest with Diksi taking the first rank in this category of characteristics.

Next step was to compute the aggregated indices for external theft protection characteristic.

	Pyaterochka	Magnit	Diksi	Ideya	811
Index	0.913	0.431	0.284	<b>0.967</b>	0.000
Rank	2	3	4	1	5
St Dev	0.025	0.064	0.146	0.027	0.000

Table 3.13. Aggregated preference indices: External Theft Protection

Next step was to compute aggregated indices for supplier fraud protection characteristic. The organizational measures in this case were valued less important than technical measures by the respondents of the survey.

We can see from Table 3.14 that Magnit store is ranked number one and that it outruns the competition quite significantly. Pyaterochka follows with rank number 2 and then Diksi and 811 are almost sharing the third rank, only Diksi outperforms 811 store by a bit. We could see from Figure X that the stores differ quite significantly in their supplier fraud protection characteristics. This characteristics shows the stores' readiness to respond to threats that come from relationships with suppliers.

	Pyaterochka	Magnit	Diksi	Ideya	811
Index	0.687	<b>1.000</b>	0.493	0.000	0.480
Rank	2	1	3	5	4
St Dev	0.072	0.000	0.035	0.000	0.038

Table 3.14. Aggregated preference indices: Supplier Fraud Protection

Next step was to compute aggregated indices for administrative error protection characteristics. The result is shown in Table 3.15 and in appendix 3 in Figures 37, 38 and 39.

	Pyaterochka	Magnit	Diksi	Ideya	811
Index	0.104	<b>0.960</b>	0.733	0.000	0.876
Rank	4	1	3	5	2
St Dev	0.085	0.033	0.055	0.000	0.101

Table 3.15. Aggregated preference indices: administrative error protection

Next step was to calculate the aggregated indices for the cyber threats protection characteristics, where the relative importance of organizational and technical measures was set up as follows:

- $w(\text{CTP organizational measures}) > w(\text{CTP technical measures})$

	Pyaterochka	Magnit	Diksi	Ideya	811
Index	0.475	<b>1.000</b>	0.475	0.000	0.480
Rank	3	1	3	4	2
St Dev	0.107	0.000	0.107	0.000	0.098

Table 3.16. Aggregated preference indices: cyber threats protection

**The final step** in this technique is to aggregate all five groups of characteristics together to compute a convoluted index for each of the stores.

The following relationships among weight coefficients were set in accordance with results that we obtained through a survey (which are presented in Table X):

- $w(\text{internal theft protection}) < w(\text{external theft protection})$
- $w(\text{supplier fraud protection}) > w(\text{cyber threats protection})$
- $w(\text{administrative error protection}) > w(\text{cyber threats protection})$
- $w(\text{administrative error protection}) < w(\text{supplier fraud protection})$

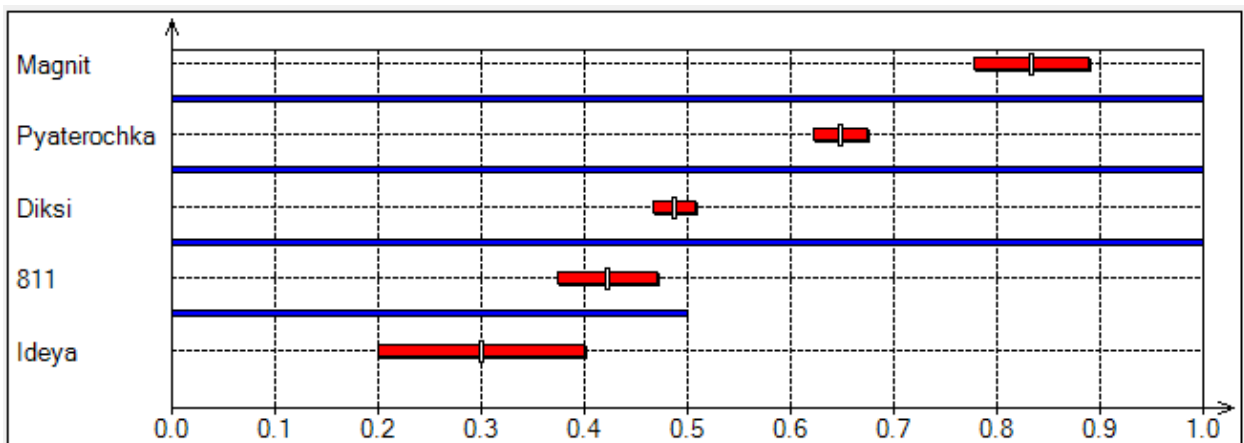


Figure 3.6. Aggregated Preference Indices: Security Index



	Pyaterochka	Magnit	Diksi	Ideya	811
Index	0.648	<b>0.834</b>	0.487	0.300	0.422
Rank	2	1	3	5	4
St Dev	0.026	0.055	0.020	0.100	0.048

Table 3.17. Aggregated preference indices: Security Index

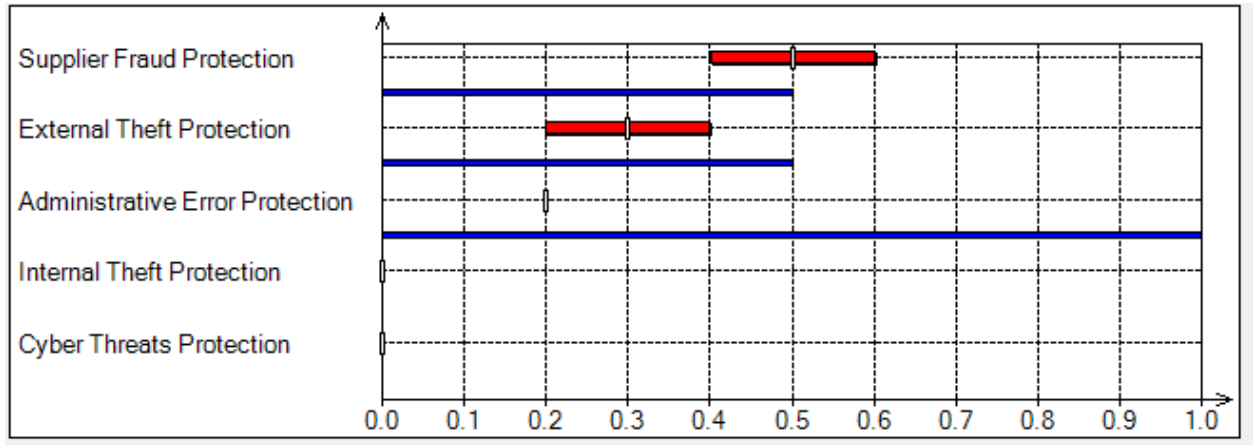


Figure 3.7. Weight-coefficients estimations visualization: Security Index

Weight of index	Min	Max	Mean	StDev	Rank
w(Internal Theft Protection)	0.0000	0.0000	0.0000	0.0000	4
w(External Theft Protection)	0.2000	0.4000	0.3000	0.1000	2
w(Supplier Fraud Protection)	0.4000	0.6000	0.5000	0.1000	1
w(Administrative Error Protection)	0.2000	0.2000	0.2000	0.0000	3
w(Cyber Threats Protection)	0.0000	0.0000	0.0000	0.0000	4

Figure 3.8. Statistics of admissible weight-coefficients values: Security index

From table 3.17 it can be seen that Magnit store has the highest overall security index, followed by Pyaterochka, Diksi, and 811 with Ideya having the lowest security index. This concludes the stage of analysis of the information with the APIS. The next stage of the framework is results analysis and it is presented in the next section, results and discussion.

Apart from the comparison of the stores and the ranking of the security index, the proposed framework allows developing specific recommendations for each store. The specific recommendations are further discussed in the next section of the thesis.

## RESULTS AND DISCUSSION

The term “security” was defined as the state of protection against threats. The threats were limited to those that result in economic losses. In order to assess security, the term security level was established in order to allow comparisons of different business entities and to help understanding of the differences among the compared business entities. Several related concepts, such as threat, risk, impact, security system and secured object were also explained in this chapter. In the second section of this chapter, the fundamentals of business entity security were discussed. Importance of organizational security was advocated and the common means of maintaining the organizational security as well as the major components of the security systems for business entities were analyzed. Current business trends, such as the market oversupply and the current globalization bring the issue of security to the forefront of list of managerial concerns. A way to classify security of an organization was presented. As Sylvie et al (2013) stated, security can be categorized into physical, personnel and information security. Levels of physical security, according to Fenelly (2016) were examined. Additionally, the basic components of a physical security system were presented. Essentials of security system elements were described, including video surveillance, access control systems, and security personnel. Personnel security was described in detail because it is an important component of maintaining the overall security of a business entity and also due to the fact that human is commonly believed to be the weakest link in security system. Indeed, 70% of information that is stolen is done by the currently employed workers of the company and it is believed that through proper training and education the number of such instances can be mitigated. Hence, the benefits of security awareness trainings are also highlighted and ethical dimensions of security are discussed. Information security specifics are also mentioned as information security is becoming more and more complex issue for organizations nowadays. Additionally the cost-benefit considerations of the security are examined.

The third section focuses on the examination of security specifics in the context of retail industry. From this section, two important categorizations are built. The first one categorizes all the existing protection measures into three categories: human, mechanical and electronic. This categorization is later used as the background information for the interviews. However the interviews have clarified this categorization and the one that is used in this thesis is a combination of the knowledge gathered though the literature research and the interviews and it is the two categories: organizational and technical. It was deemed sufficient to group all the means of protection into two categories because recently electronic and mechanical protection measures have merged closely together and it will be hard to distinguish between the two or else to put a certain measure of protection into a specific category and therefore the mentioned categorization

of the protective measures is used. Another important classification that is the result of section 3 of this chapter is classification of the sources of threats that lead to the economic losses in retail industry.

Chapter 1 ends with section 1.4 in where the results of the interviews are described, identifying every element of the each branch of the hierarchy. As the result of chapter 1, the hierarchic system of criteria is established based on scientific literature research and practical experience.

The chapter ends with the hierarchic system of criteria which could be used for the analysis of any set of retail outlets of comparable size and employee count. The criteria of the size of the store, or its physical structure and the employee count was disregarded in the formation of the hierarchic system of indicators because the hierarchy was initially designed for the application of a set of retail outlets that are of comparable size and employee counts. Remaining criteria of security system assessment have originated from either literature review or in-depth interviews.

In the second chapter, the author described the research methodology of the current research, compared the methods possibly relevant for the solution of the problem of security system assessment and chose the most suitable method. To some extent it is a matter of the taste and the author's expertise and previous knowledge about the methods, however the argumentation for the choice of the method was intended to be as clear as possible. To summarize it, the combination of the characteristics of APIS method is what made it the most suitable method of analysis for this particular problem by this particular researcher. Perhaps the problem could be analyzed with a different method as well, but from the point of view of the author of this thesis it will produce unwanted drawbacks.

In the last section of the second chapter, the developed framework is presented and described. The framework represents a series of stages which are, if conducted in this order and according to all the guidelines listed by the author, will provide a tool for security system assessment of the business entity. In this work however the author shows how to apply the framework on the 5 case retail outlets. In order to clarify how the framework can be applied, please take a look at the Table 3.18.

In Chapter 3 the author presents a protocol of framework application, recording and explaining every step of the process of framework application. Five stores' security systems were assessed using the framework developed. The stores are Magnit, Diksi, Ideya, 811 and Pyaterochka; all five stores represent grocery retail chains, and one stores of the chain was picked for analysis in each of the five cases.

First result that we could easily understand from the analysis of data with APIS is the ranking of the stores according to the level of security. The ranking is as follows:

1. Magnit
2. Pyaterochka
3. Diski
4. 811
5. Ideya

These findings tell us that Magnit has the highest security level and is the most protected from losses store, while the Ideya has the lowest security level and is the least protected store of all the five considered in the analysis. Pyaterochka is ranked number 2, thus its security level is pretty high as well, relative to other stores like 811 and Ideya. Diski has the medium security level.

Apart from this finding, each store results may be analyzed in detail in order to understand the particular weak elements of the security system of a particular store. For instance, if we take Magnit that scored number 1 in terms of overall security system performance, we could see that this does not mean that Magnit has nothing to improve. In fact, the results that are given out by the APIS software allow us to see exactly which element of the security system has some problems. If we take a look at the APIS results for one level lower, we could easily detect the weak elements. Magnit, which scored top in terms of overall security is actually the on the last fifth place in terms of technical measures that are geared towards internal theft protection. Therefore we could say that Magnit has to look at the technical measures of the internal theft protection and this will most likely improve its overall security. Moreover, it can be seen that Magnit has weak CCTV and weak organizational protection measures from external theft. So it looks like the strong areas of Magnit are administrative error protection, supplier fraud protection and cyber threat protection. However external theft and internal theft seem to be the threats for Magnit. If the management would like to know what specifically can be done in order to combat these issues, to improve these weak elements of the Magnit store, it can be also easily done by further analyzing the APIS. So, the CCTV of Magnit should be improved with the specific focus on the degree of integration of the systems because Magnit didn't score high on that. It seems that the CCTV currently installed in the store is poorly integrated with other system, so perhaps investing in the CCTV upgrade or its renewal will benefit the overall security of the Magnit store. Similarly, in order to improve the protection from external theft, the results suggest that Magnit should focus on customer awareness programs development, on the formation of rapid response team, on creation of the new position of loss prevention specialist in the store, and on training of the security guards. In order to improve the protection from the

internal theft, the focus of Magnit should be on cashier control system upgrade, labor hours control system upgrade and burglar alarm system upgrade.

As presented in Table 3.18, in order to apply the framework in the context of retail outlets, for example if there is a different set of retail outlets and the goal is to analyze the security system of such outlets, only the last three stages of the framework will have to be redone, because the developed hierarchic system of indicators as well as the importance of criteria gathered through the survey of experts will be still valid for other retail outlets. It may be argued that the development of these criteria is the only contribution of this work, however the author would like to propose a claim that the developed hierarchical system of indicators for retail outlets is not the only thing that the author is contributing in this work. The contribution of this work is actually greater because it produced a framework that could be repeated from the beginning to the end and that will give results for any business entity regardless of the industry. Therefore the application of the framework is more broad than just the developed hierarchic system of criteria, although the development of the hierarchic system of criteria is also the contribution of the work.

Table 3.18. Framework application in various context (Author, 2017)

	For application in <i>retail</i> context	For application in <i>non- retail</i> context
Criteria identification (interviews, literature)	-	X
Hierarchic system of indicators formation	-	X
Importance of criteria assessment (survey of experts)	-	X
Criteria evaluation (experts opinion)	X	X
Analysis of data with APIS	X	X
Analysis of results and recommendations formulation	X	X

The developed framework allows to assess the store's security system current performance in relation to other stores, and also to understand the individual value of the security system, which can be also compared after a certain period of time during the repeated assessment. The developed framework allows to identify weak elements of the security system as it was shown in the example of the five case retail outlets, and allows to develop specific recommendations based on the results of the calculations as it was shown on the Magnit example. This allows focusing the attention of the managers on the specific elements of the

security system, increases the knowledge about the current state of the security system and allows to make the first step towards losses minimization. After the recommendations that are formulated through framework application are followed and applied, the security level will increase, which in turn will produce smaller losses realized by the store and the minimization of losses is an important direction for management of retail outlets as confirmed by both theory and practice. Therefore the developed framework is important for the community of retail managers, security system sellers, security system developers and managers of other business entities as well, because the framework can be also applied in a non-retail context.

## CONCLUSION

A comprehensive framework of security system assessment was developed and applied in retail context in this thesis. Chapter 1 focused on the development of the list of criteria, through identification of the definitions related to the problem of security, exploration of the problem of security in the context of business entities, and finally, through specification of the knowledge related to the problem of security in retail. The chapter ends with a hierarchical system of criteria that were specifically developed for application in the context of assessing retail outlets of comparable size and employee count. In Chapter 2, the methodology of the work was described as well as various methods that thought to be applicable in the context of solving the problem of security assessment. The method for the analysis of information was chosen to be APIS, because the author believes that this method is the most suitable for the current problem as it has a unique combination of characteristics. After the framework was established in section 2.3 it was then applied on a real life example of the five retail outlets. The results of this thesis can be summarized as follows:

- The criteria for security system assessment were developed on the basis of scientific literature and practical experience analysis in Chapter 1
- The framework of security system assessment for retail outlets was developed and formulated on the basis of selected criteria and quantitative evaluation of the questionnaire results in Chapter 2
- The framework was applied on the selected case outlets in order to test the framework and provide evidence of its applicability in Chapter 3

As the result of the framework application, each of the retail outlets were given a snapshot of the current situation with its security system, all the weak and strong elements of the stores' security system were identified and then the recommendations were formulated based on the analysis of the calculations. The framework is applicable in both retail context and non-retail context with the difference presented in Table 3.X.

The theoretical contribution of this work is primarily the development of a universal framework of security system assessment, and additionally is the development of the hierarchic system of criteria of security system assessment, which will be valid for the comparison of any set of retail outlets of comparable size and employee count. Additionally, the theoretical contribution is the weights that the experts assigned to each of the criteria; these may be also used for the repetition of the framework application in retail context. Moreover, it was shown that the framework can be straightforwardly and successfully applied, therefore showing that the developed framework works in the specified context. The theoretical contribution of this work is

mainly the identification of key elements characterizing the process of security system assessment. Additionally, it is also valuable because it combines the existing knowledge on the topic of security in retail and summarizes it in a unique fashion.

The practical contribution of this work lies in the development of the framework that can be regarded as a series of stages, the consecutive execution of which provides a thorough assessment model for security assessment. The framework was designed to be applicable in the context of various industries, however in the following thesis it was tailored to the context of retail industry and applied on grocery retail outlets. This framework can be taken and applied in diverse context, if all the stages are properly followed. The framework is applicable to any type of retail business and for the application on a different type of retail business the first stages of the framework and the developed hierarchic system of criteria will remain the same. However if the management would like to apply the framework in the context of another type of business entity it is also possible, only the hierarchic system of criteria will have to be remodeled and tailored to the specifics of a particular type of business entity. Therefore it can be said that the developed framework is a flexible and universal tool for managers. The development of this framework is important for managers because currently there is no widely accepted framework of security system assessment for retail outlets. The developed framework allows to identify which store has better security and which stores have lower security level. Not only it allows to compare the outlets, but also it allows to identify the weak and the strong points in order to know which elements to focus on when developing the program for the improvement of security level.

To summarize, the contribution of this thesis is:

- Development of the list of criteria (universal in retail context)
- Formation of the hierarchic system of criteria (universal in retail context)
- Assessment of the weights of each criteria (universal in retail context)
- Development of the important and relevant framework of security system assessment (currently there is no widely accepted framework)
- Illustration of the framework's applicability.



## REFERENCES

1. Azapagic, Adisa, and Slobodan Perdan. "An integrated sustainability decision-support framework Part II: Problem analysis." *International Journal of Sustainable Development & World Ecology* 12, no. 2 (2005): 112-31.
2. Beck, Adrian. "Automatic product identification & shrinkage: Scoping the potential." *Efficient Consumer Response Europe*, February 2002.
3. Beck, Adrian, and Walter Palmer. "The Importance of Visual Situational Cues and Difficulty of Removal in Creating Deterrence: The Limitations of Electronic Article Surveillance Source Tagging in the Retail Environment." *Journal of Applied Security Research* 6, no. 1 (2010): 110-23.
4. Bellini, Silvia, Maria Grazia Cardinali, and Benedetta Grandi. "A structural equation model of impulse buying behaviour in grocery retailing." *Journal of Retailing and Consumer Services* 36 (2017): 164-71.
5. Belton, Valerie, and Tony Gear. "On a short-coming of Saaty's method of analytic hierarchies." *Omega* 11, no. 3 (1983): 228-30.
6. Bresz, F. P. "People – often the weakest link in security, but one of the best places to start: without awareness and training, security compliance is not possible." *Journal of Health Care Compliance* 6, no. 4 (2004): 57-61.
7. Briggs, Rachel, Charlie Edwards, and Julie Pickard. *The business of resilience: corporate security for the 21st century*. London, England: Demos, 2006.
8. Butov, A. "Grocery retail market." *Higher School of Economics Research Institute*, 2016, 1-60.
9. Campbell, Jamonn, Nathan Greenauer, Kristin Macaluso, and Christian End. "Unrealistic optimism in internet events." *Computers in Human Behavior* 23, no. 3 (2007): 273-284.
10. Das, I., and J. E. Dennis. "A closer look at drawbacks of minimizing weighted sums of objectives for Pareto set generation in multicriteria optimization problems." *Structural Optimization* 14, no. 1 (1997): 63-69.
11. Dicarlo, Jennifer. "Industry Specific Q&A: Loss Prevention/Retail Security." *Women in the Security Profession*, 2017, 227-31.
12. Dulyakorn, Nitikorn, Chavana Pavaganun, Benja Mangalabruks, Yusaku Fujii, and Preechap. Yupapin. "BOB Loss-preventing for Modern Trade Retail Product Safety." *Procedia Engineering* 8 (2011): 353-59.
13. Egorova, L. S., P. S. Frolova, and O. N. Frolova. "Risks and threats in organization's personnel security system." *Bulletin of N.A. Nekrasov's KSU* 6 (2013): 144-48.

14. Fennelly, Lawrence J. *Effective physical security*. Cambridge, MA: Elsevier, 2016.
15. Fernie, John, Sue Fernie, and Christopher M. Moore. *Principles of retailing*. Abingdon, Oxon: Routledge, Taylor & Francis Group, 2015.
16. Ficht, L., and J. Levashina. "When lying, cheating and stealing is not necessarily illegal: the need to adopt a commercial fraud standard in employment law cases." *Southern Law Journal* 21, no. 2 (2011), 289-307.
17. Firesmith, D. G. *Analyzing and specifying reusable security requirements*. New York: Carnegie Mellon University, 2003.
18. Ford, Robert C., Gary P. Latham, and Gwen Lennox. "Mystery shoppers: a new tool for coaching employee performance improvement." *Organizational Dynamics* 40, no. 3 (2011): 157-64.
19. Garcia, Mary Lynn. *The design and evaluation of physical protection systems*. Amsterdam: Elsevier/Butterworth-Heinemann, 2008.
20. Greggo, Alan, and Millie Kreseovich. *Retail security and loss prevention solutions*. Boca Raton: Taylor & Francis, 2016.
21. Grewal, Dhruv, and A. L. Roggeveen. "The Future of Retailing." *Journal of Retailing* 93, no. 1 (2017): 1-6.
22. Grigoryeva V. V., Gorkovenko E. V., Platonova I. V., Borshevskaya E. P., Makrinova E. I. Formation of Concept of Provision of Economic Security of Organization: Personnel Aspect. *European Research Studies*. no. 2 (2016): 46-54.
23. Halibozeck, Edward P., and Gerald L. Kovavich. *The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program*. Elsevier Butterworth-Heinemann, 2017.
24. Haufe, Knut, Ricardo Colomo-Palacios, Srdan Dzombeta, Knud Brandis, and Vladimir Stantchev. "Security Management Standards: A Mapping." *Procedia Computer Science* 100 (2016): 755-61.
25. Healy, Richard J., and Timothy J. Walsh. *Industrial security management; a cost-effective approach*. New York: American Management Association, 1971.
26. Holston, C., and B. Kleiner. "Excellence in reward systems." *Culture and Religion Review Journal* 2015, no. 3 (2015): 54-61.
27. Hovanov, Nikolai, Maria Yudaeva, and Kirill Hovanov. "Multicriteria estimation of probabilities on basis of expert non-numeric, non-exact and non-complete knowledge." *European Journal of Operational Research* 195, no. 3 (2009): 857-63.
28. Hwang, C., and K. Yoon. *Multi Attribute Decision Making: Methods and Applications*. New York: Springer-Verlag, 1981.

29. Inman, J. Jeffrey, and Hristina Nikolova. "Shopper-Facing Retail Technology: A Retailer Adoption Decision Framework Incorporating Shopper Attitudes and Privacy Concerns." *Journal of Retailing* 93, no. 1 (2017): 7-28.
30. Janeiro, L., and Martin K. Patel. "Choosing sustainable technologies. Implications of the underlying sustainability paradigm in the decision-making process." *Journal of Cleaner Production* 105 (2015): 438-46.
31. Ishenko, Nikolay. "Major grocery chains have gained market share". *Vedomosti* 4, 2015, 13-21
32. Kim, I., and O.I. De Weck. "Adaptive weighted-sum method for bi-objective optimization: Pareto front generation." *Structural and Multidisciplinary Optimization* 29, no. 2 (2005): 149-58.
33. Knežević, Blaženka, Mia Delić, and Marko Jurčević. "Detecting and Preventing Employee's Theft in Retail." *Proceedings of International Scientific Conference*, 2016, 90-104.
34. Knight, Paul Emerson., and Alan M. Richardson. *The scope and limitation of industrial security*. Springfield, IL: Thomas, 1963.
35. Koh, R., N. Lam, M. Dinning, and E. Shuster. "Prediction, Detection, and Proof: An Integrated Auto-ID Solution to Retail Theft." *Massachusetts institute of technology*, 2003, 1-16.
36. Lincke, Susan. *Security planning: an applied approach*. Cham: Springer International Publishing, 2015.
37. Lowrance, William W. "Of Acceptable Risk: Science and the Determination of Safety." *Journal of The Electrochemical Society* 123, no. 11 (1976).
38. Mandelbaum, Albert Joseph. *Fundamentals of protective systems; planning, evaluation, selection*. Springfield, IL: Charles C. Thomas, 1973.
39. Marcum, C. Everett. *Security Priorities and Essential Protection*. *Mimeographed manuscript*. Safety Studies Department, West Virginia University, 1979.
40. Mattsson, Jan. "Strategic insights from mystery shopping in B2B relationships." *Journal of Strategic Marketing* 20, no. 4 (2012): 313-22.
41. Mccrohan, Kevin F., Kathryn Engel, and James W. Harvey. "Influence of Awareness and Training on Cyber Security." *Journal of Internet Commerce* 9, no. 1 (2010): 23-41.
42. "Merriam-Webster dictionary." Merriam-Webster. Accessed March 19, 2017. <https://www.merriam-webster.com/>.

43. Millman, René. "Four in ten security staffers write down passwords." SC Media US. August 27, 2007. Accessed March 19, 2017. <https://www.scmagazine.com/four-in-ten-security-staffers-write-down-passwords/article/551819/>.
44. Ministry of Interior. "Ministry of Interior Guideline Document N78.36.003-2002." Corporate Security and Safety Market in Russia. 2015. Accessed March 13, 2015. <https://www.tekes.fi/globalassets/global/>.
45. Mittal, K. C., and A. Prashar. "A Field study on opportunities and challenges faced by organized retailers in tri-city." *Tecnia Journal of Management Studies* 57 (2011).
46. Newman, Jerry M., Barry A. Gerhart, and George T. Milkovich. *Compensation*. New York, NY: McGraw-Hill Education, 2017.
47. "Oxford Dictionary." Oxford Dictionaries | English. Accessed March 18, 2017. <https://en.oxforddictionaries.com/>.
48. Petruzzi, John, and Rachelle Loyear. "Improving organizational resilience through enterprise security risk management." *Journal of Business Continuity and Emergency Planning* 10, no. 1 (2016): 44-56.
49. Post, Richard S., Arthur A. Kingsbury, and David A. Schachtsiek. *Security administration: an introduction to the protective services*. Boston: Butterworth-Heinemann, 1991.
50. Pretious, Mike, Robert Stewart, and David Logan. "Retail security: a survey of methods and management in Dundee." *International Journal of Retail & Distribution Management* 23, no. 9 (1995): 28-35.
51. Schmallegger, Frank. *Criminal justice a brief introduction*. Pearson Education Prentice Hall, 2013.
52. Reid, Robert N. *Guards and guard forces. Facility Manager's Guide to Security: Protecting Your Assets*, The Fairmont Press, 2005.
53. Stewart, Tj. "A critical survey on the status of multiple criteria decision making theory and practice." *Omega* 20, no. 5-6 (1992): 569-86.
54. Stone, Michele. "Interview with Mischelle Stone." *Journal of Applied Security Research* 3, no. 1 (2007): 113-22.
55. Sylvie, Johnatan R., S. R. Thomas, S. Lee, R. E. Chapman, and R. T. Smith. "Development and Interpretation of the Security Rating Index." *Journal of Construction Engineering and Management* 139, no. 2 (2013): 185-94.
56. Systems, Inc. Checkpoint. "Global Retail Theft Barometer." Global Retail Theft Barometer. Accessed March 28, 2017. <http://www.globalretailtheftbarometer.com/>.

57. Talbot, Julian, and Miles Gareth. Jakeman. *Security risk management body of knowledge*. Vol. 69. Hoboken, NJ: John Wiley & Sons, 2009.
58. Tam, L., M. Glassman, and M. Vandenwauver. "The psychology of password management: a tradeoff between security and convenience." *Behaviour & Information Technology* 29, no. 3 (2010): 233-44.
59. Triantaphyllou, Evangelos, and Chi-Tun Lin. "Development and evaluation of five fuzzy multiattribute decision-making methods." *International Journal of Approximate Reasoning* 14, no. 4 (1996): 281-310.
60. Triantaphyllou, Evangelos. "Multi-Criteria Decision Making Methods." *Applied Optimization Multi-criteria Decision Making Methods: A Comparative Study* 44 (2000): 5-21.
61. Turban, Efraim, and Linda Volonino. *Information technology for management: transforming organizations in the digital economy*. Hoboken (NJ): J. Wiley, 2012.
62. Tyska, Louis A., Lawrence J. Fennelly, and Ed San Luis. *Office and office building security*. Boston: Butterworth-Heinemann, 1994.
63. Ura, Dasho Karma. *Asian business and management practices: trends and global considerations*. Hershey: Business Science Reference, 2015.
64. Uraic, Henry S., and Leroy Pagano. *Security management systems*. Springfield, IL: Thomas, 1974.
65. Verizon. "Verizon Data Breach Investigation Report: Understand Your Cybersecurity Threats." Verizon Enterprise Solutions. 2017. Accessed May 28, 2017. <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>.
66. Wathen, Thomas W. *Security subjects: an officers' guide to plant protection*. Springfield, IL: Charles C. Thomas, 1972.
67. Woodruff, Ronald S. *Industrial Security Techniques*. Columbus, OH: Charles E. Merrill Publishing Co., 1974.
68. Wu, Yu Andy, Carl S. Guynes, and John Windsor. "Security Awareness Programs." *Review of Business Information Systems* 16, no. 4 (2012): 165.

## APPENDICES

### Appendix 1. Questionnaire results: relative importance of characteristics

	1	2	3	4	5	6	7	8	9	10	11	12	Average
<b>Internal Theft Protection</b>	<b>25</b>	<b>25</b>	<b>27</b>	<b>30</b>	<b>35</b>	<b>25</b>	<b>10</b>	<b>10</b>	<b>25</b>	<b>25</b>	<b>20</b>	<b>25</b>	<b>24</b>
<b>Organizational Measures</b>	<b>50</b>	<b>60</b>	<b>55</b>	<b>70</b>	<b>45</b>	<b>60</b>	<b>65</b>	<b>85</b>	<b>75</b>	<b>70</b>	<b>50</b>	<b>60</b>	<b>62</b>
Rewards system	2	1	3	4	2	3	4	5	2	1	3	2	<b>3</b>
Pre-employment screening	1	1	2	1	1	1	2	1	1	2	1	1	<b>1</b>
Awareness programs	4	2	1	1	1	2	3	1	2	1	2	2	<b>2</b>
Internal audits	4	3	2	5	4	4	3	5	4	2	6	4	<b>4</b>
Mystery shopping	4	3	2	5	3	2	2	3	4	3	2	3	<b>3</b>
Security team work	5	4	6	5	3	7	5	5	5	4	6	5	<b>5</b>
Customers involvement	2	3	3	4	2	4	3	3	3	4	2	3	<b>3</b>
Employees education	5	4	4	4	3	5	4	3	5	4	3	4	<b>4</b>
Polygraph control	6	4	5	3	6	5	5	3	4	5	5	5	<b>5</b>
Collective liability	1	2	1	1	2	1	1	1	1	2	1	1	<b>1</b>
<b>Technical Measures</b>	<b>50</b>	<b>40</b>	<b>45</b>	<b>30</b>	<b>55</b>	<b>40</b>	<b>35</b>	<b>15</b>	<b>25</b>	<b>30</b>	<b>50</b>	<b>40</b>	<b>38</b>
Cashier control system	4	3	5	6	5	4	6	5	5	3	5	4	<b>5</b>
Labor hours control system	2	6	4	3	5	4	3	4	4	3	4	4	<b>4</b>
Access control system	3	2	3	4	5	3	2	1	6	5	3	3	<b>3</b>
CCTV system	4	3	4	3	5	3	3	4	4	4	2	4	<b>4</b>
Burglar alarm system	1	1	1	1	2	1	1	2	1	1	1	1	<b>1</b>
Mirrors	2	1	2	1	2	3	3	2	1	2	3	2	<b>2</b>
<b>External Theft Protection</b>	<b>25</b>	<b>30</b>	<b>36</b>	<b>20</b>	<b>25</b>	<b>30</b>	<b>30</b>	<b>25</b>	<b>25</b>	<b>35</b>	<b>30</b>	<b>30</b>	<b>28</b>
<b>Organizational measures</b>	<b>15</b>	<b>40</b>	<b>50</b>	<b>40</b>	<b>35</b>	<b>15</b>	<b>45</b>	<b>25</b>	<b>25</b>	<b>30</b>	<b>50</b>	<b>30</b>	<b>33</b>
Customer awareness programs	2	3	1	3	1	2	2	2	3	1	2	2	<b>2</b>
Loss prevention specialist	5	4	3	5	6	7	5	3	4	5	5	5	<b>5</b>
Security guard	1	1	1	2	1	1	2	1	1	1	1	1	<b>1</b>

Rapid response team	2	1	2	3	1	2	3	2	2	2	2	1	<b>2</b>
Lawsuits handling	1	2	3	1	2	2	1	3	1	2	2	3	<b>2</b>
<b>Technical measures</b>	85	60	50	60	65	85	55	75	75	70	50	70	<b>67</b>
EAS													
Passage width	2	3	1	1	2	1	2	3	2	2	2	1	<b>2</b>
Tag detection probability	2	3	2	2	3	3	4	3	3	4	2	3	<b>3</b>
Forced activation possibility	3	1	2	5	3	4	2	3	3	3	3	4	<b>3</b>
CCTV													
Cameras resolution	4	2	4	4	3	4	4	6	4	4	2	4	<b>4</b>
Archive depth	3	2	4	3	4	2	3	2	1	3	2	3	<b>3</b>
Movement detection	4	3	5	4	4	4	2	4	6	3	5	4	<b>4</b>
Pre-alarm function	5	2	4	3	3	4	4	4	3	4	4	6	<b>4</b>
Degree of integration	2	4	6	4	3	5	4	2	3	4	2	6	<b>4</b>
Face recognition	4	2	4	6	4	3	4	4	4	2	4	5	<b>4</b>
Burglar alarm	3	4	2	3	3	3	4	2	3	3	3	3	<b>3</b>
Mirrors	1	2	1	2	2	3	2	3	1	2	2	2	<b>2</b>
<b>Supplier Fraud Protection</b>	<b>20</b>	<b>15</b>	<b>17</b>	<b>20</b>	<b>10</b>	<b>15</b>	<b>25</b>	<b>25</b>	<b>20</b>	<b>20</b>	<b>20</b>	<b>20</b>	<b>19</b>
<b>Organizational measures</b>	15	35	15	45	25	30	45	55	40	30	15	20	31
Goods receipt regulations	5	4	5	4	4	5	6	4	5	5	5	5	<b>5</b>
<b>Technical measures</b>	85	65	85	55	75	70	55	45	60	70	85	80	69
CCTV	4	3	4	4	5	4	4	4	3	5	4	4	<b>4</b>
Goods receipt control	4	4	4	3	4	4	5	4	4	2	6	4	<b>4</b>
Barcodes scanners	3	2	5	4	3	2	3	3	4	2	3	3	<b>3</b>
Video-logistics systems	4	4	2	6	2	4	4	4	3	4	4	4	<b>4</b>
Sealing and transportation rules	3	2	5	2	3	3	3	3	4	2	3	3	<b>3</b>
<b>Administrative Errors Protection</b>	<b>20</b>	<b>20</b>	<b>10</b>	<b>15</b>	<b>10</b>	<b>15</b>	<b>25</b>	<b>25</b>	<b>10</b>	<b>15</b>	<b>15</b>	<b>15</b>	<b>16</b>
<b>Organizational measures</b>	85	65	85	65	75	70	75	45	60	70	90	80	72
Documentation regulations	3	2	3	3	3	3	2	4	2	4	1	4	<b>3</b>

ABC analysis	3	2	3	4	2	3	3	3	3	2	4	3	<b>3</b>
Conversion	3	2	1	3	4	2	3	3	3	3	3	3	<b>3</b>
<b>Technical measures</b>	<b>15</b>	<b>35</b>	<b>15</b>	<b>35</b>	<b>25</b>	<b>30</b>	<b>25</b>	<b>55</b>	<b>40</b>	<b>30</b>	<b>10</b>	<b>20</b>	<b>28</b>
System of document flow	3	4	2	5	4	2	3	1	2	3	4	3	
Automated controls	4	3	4	3	4	5	3	5	3	3	4	4	<b>4</b>
CCTV	2	3	2	1	1	2	3	5	2	1	2	2	<b>2</b>
Lines control system	3	4	2	4	2	3	3	3	3	4	2	3	<b>3</b>
Regulations control	4	5	2	4	3	5	2	5	4	4	4	4	<b>4</b>
Customers count	2	1	2	1	2	3	4	2	1	2	1	2	<b>2</b>
Face recognition system	4	3	4	3	3	6	4	3	2	5	3	2	<b>4</b>
<b>Cyber threats protection</b>	<b>10</b>	<b>10</b>	<b>10</b>	<b>15</b>	<b>20</b>	<b>15</b>	<b>10</b>	<b>15</b>	<b>20</b>	<b>5</b>	<b>15</b>	<b>10</b>	<b>13</b>
<b>Organizational measures</b>	<b>55</b>	<b>65</b>	<b>55</b>	<b>65</b>	<b>65</b>	<b>55</b>	<b>50</b>	<b>60</b>	<b>55</b>	<b>50</b>	<b>80</b>	<b>80</b>	<b>61</b>
Vulnerability tests	3	2	1	3	3	4	2	5	3	2	1	5	<b>3</b>
Employees training	2	3	1	4	3	1	2	3	1	1	2	3	<b>3</b>
Management	2	1	2	3	4	1	2	1	2	2	3	2	<b>2</b>
<b>Technical measures</b>	<b>45</b>	<b>35</b>	<b>45</b>	<b>35</b>	<b>35</b>	<b>45</b>	<b>50</b>	<b>40</b>	<b>45</b>	<b>50</b>	<b>20</b>	<b>20</b>	<b>39</b>
Protection mechanisms	3	1	3	2	1	4	3	3	3	2	3	4	<b>3</b>



## Appendix 2. Questionnaire: relative importance of characteristics



**Graduate  
School of Management**  
St. Petersburg State University

### **Questionnaire for security system experts.**

**Dear respondent!**

This survey is undertaken as a part of master thesis project for the Graduate School of Management.

The data will be collected for the purpose of developing a balanced and comprehensive method of security system assessment of retail outlets through identification of relative importance of previously established characteristics of security.

The arranger of the research ensures confidentiality of the information you will provide as the results of this survey will be used in cumulative form only.

**Please read the instructions carefully and follow them in order to ensure proper filing of the survey and further acceptance of the results obtained into processing stage.**

*Please answer the following questions:*

Each retail outlet is represented by a number of characteristics. The questions will follow the order of these characteristics level by level from top to bottom.

At the highest layer, five groups of characteristics are identified

- Internal Theft Protection
- External Theft Protection
- Supplier Fraud Protection
- Administrative Error Protection
- Cyber Threats Protection

1. Spread 100 points between five groups of characteristics presented above according to their relative importance, with more points indicating more important characteristics.

Group of Characteristics	Scores
Internal Theft Protection	
External Theft Protection	
Supplier Fraud Protection	
Administrative Error Protection	
Cyber Threats Protection	

2. One level down, each of these five groups of characteristics is divided into organizational and technical measures. Please spread 100 points between organizational and technical measures for each of the five groups of characteristics, according to their relative importance in security system assessment process.

	Internal Theft Protection	External Theft Protection	Supplier Fraud Protection	Administrative Error Protection	Cyber Threats Protection
Organizational measures					
Technical measures					

For the next questions, please rate the importance of characteristics with a 7-point scale according to the degree of influence of these characteristics on an overall security of a retail outlet.

3. Please rate the characteristics of internal theft protection, organizational measures, with a 7-point scale, 7 representing it has a definite impact and 1 being it has little to no impact.

Characteristics	Scores
Rewards system	
Pre-employment screening	
Awareness programs	
Internal audits	
Mystery shopping	
Security team work	
Customers involvement	
Employees education	
Polygraph control	
Collective liability	

4. Please rate the characteristics of internal theft protection, technical measures, with a 7-point scale, 7 representing it has a definite impact and 1 being it has little to no impact.

Characteristics	Scores
Cashier control system	
Labor hours control system	
Access control system	
CCTV system	
Burglar alarm system	

5. Please rate the characteristics of external theft protection, organizational measures with a 7-point scale, 7 representing the characteristic has a definite impact on security of the store and 1 representing the characteristic has little to no impact.

Characteristics	Scores
Customer awareness programs	
Loss prevention specialist	
Security guard	
Rapid response team	
Lawsuits handling	

Please rate characteristics of external theft protection, technical measures with a 7-point scale, 7 representing the characteristic has a definite impact on security of the store and 1 representing the characteristic has little to no impact.

Characteristics	Scores
EAS	
CCTV	
Burglar alarm	
Mirrors	

6. Please rate CCTV sub-characteristics on a 7-point scale, 7 representing definite impact on the security of the store and 1 representing little to no impact on the security of the store.

Characteristics	Scores
Cameras resolution	
Archive depth	
Movement detection	
Pre-alarm function	
Degree of integration	
Face recognition	

7. Please rate EAS sub-characteristics on a 7-point scale, 7 representing definite impact on the security of the store and 1 representing little to no impact on the security of the store.

Characteristics	Scores
Passage width	
Tag detection probability	
Forced activation possibility	

8. Please rate supplier fraud protection sub-characteristics on a 7-point scale, 7 representing definite impact on the security of the store and 1 representing little to no impact on the security of the store.

Characteristics	Scores
Goods receipt regulations	
CCTV	
Goods receipt control	
Barcodes scanners	
Video-logistics systems	
Sealing and transportation rules	

9. Please rate cyber threat protection sub-characteristics on a 7-point scale, 7 representing definite impact on the security of the store and 1 representing little to no impact on the security of the store.

Characteristics	Scores
Vulnerability tests	
Employee training	
Management	

Your answers are very important to the organizer of this study and successful completion of the research.

Please feel free to contact the organizer of the study if you would like to receive more information on the project, have questions about how the information will be stored, or have additional feedback related to the subject of the study.

Marina Syromyatnikova

mob.: +7-921-xxx-xx-xx

e-mail: [marinaxxxxxxx@xxx.com](mailto:marinaxxxxxxx@xxx.com)

Please also provide your contact information as well as brief information about yourself in the space below. You may be contacted to clarify the answers.

Name: \_\_\_\_\_

Occupation: \_\_\_\_\_

e-mail: \_\_\_\_\_

Mobile phone: \_\_\_\_\_

**Thank you for your participation in the survey!**

### Appendix 3. Additional Output from APIS

#### Internal Theft Protection: Technical measures

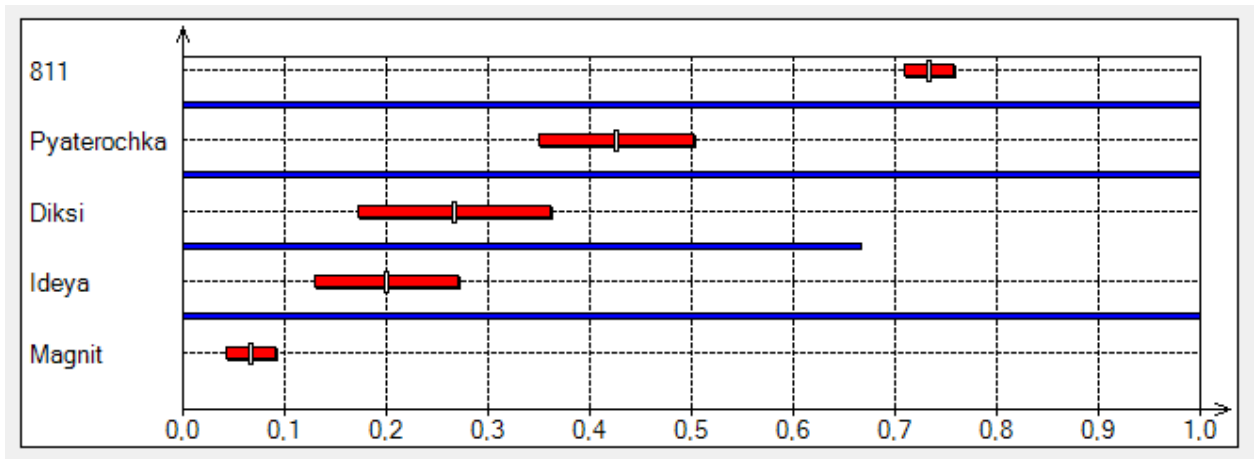


Figure 1. Aggregated preference indices visualization for “internal theft protection: technical measures” characteristic

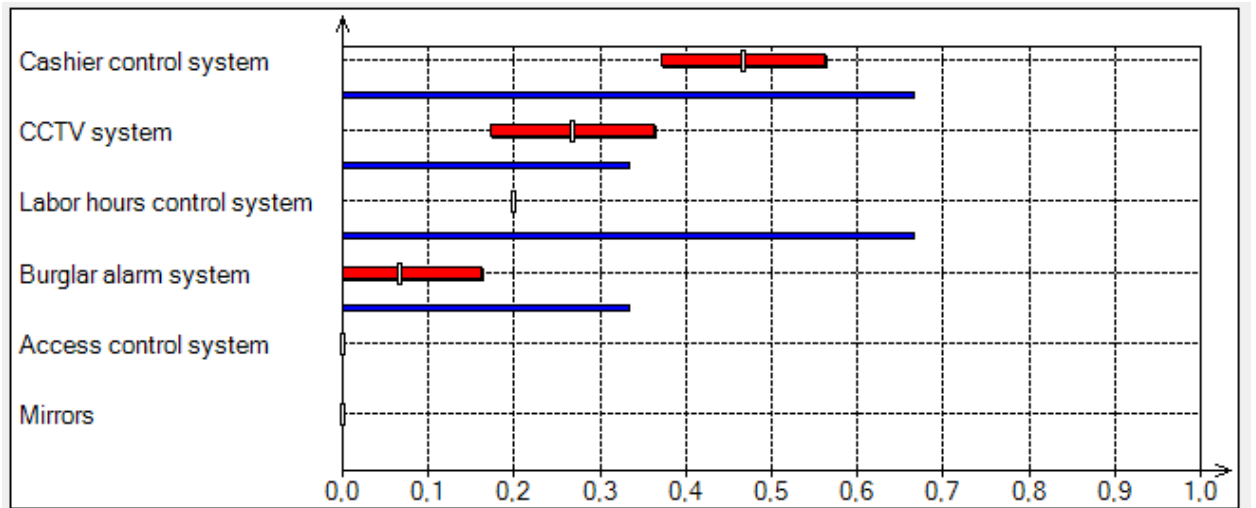


Figure 2. Weight-coefficients estimations visualization for “Internal Theft Protection: Technical Measures” characteristic

Weight of index	Min	Max	Mean	StDev	Rank
w(Cashier control system)	0,4000	0,6000	0,4667	0,0943	1
w(Labor hours control system)	0,2000	0,2000	0,2000	0,0000	3
w(Access control system)	0,0000	0,0000	0,0000	0,0000	5
w(CCTV system)	0,2000	0,4000	0,2667	0,0943	2
w(Burglar alarm system)	0,0000	0,2000	0,0667	0,0943	4
w(Mirrors)	0,0000	0,0000	0,0000	0,0000	5

Figure 3. Statistics of admissible weight-coefficients values for internal theft protection: technical measures

## External theft protection: organizational measures

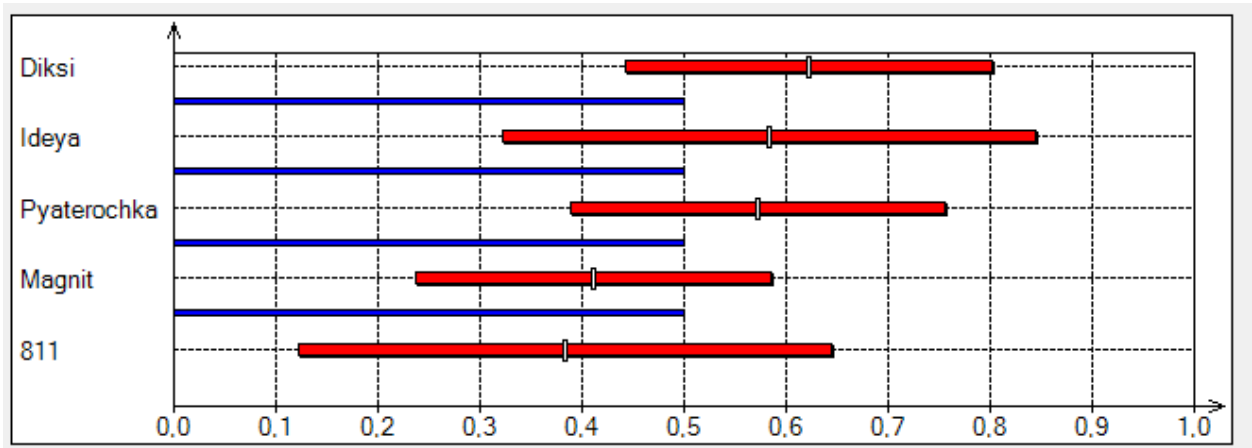


Figure 4. Aggregated preference indices visualization for “external theft protection: organizational measures”.

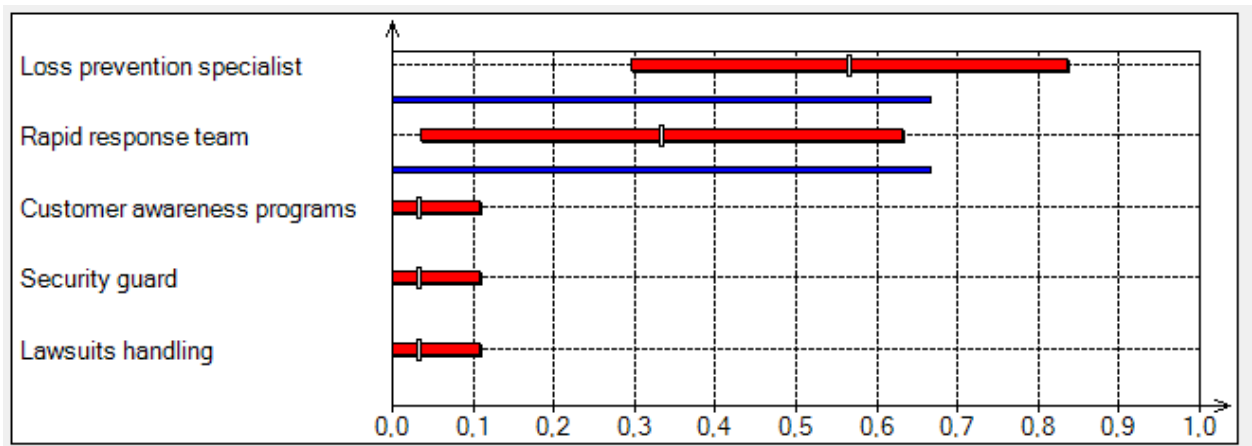


Figure 5. Weight-coefficients estimations visualization for “external theft protection: organizational measures”.

Weight of index	Min	Max	Mean	StDev	Rank
w(Customer awareness programs)	0,0000	0,2000	0,0333	0,0745	3
w(Loss prevention specialist)	0,2000	1,0000	0,5667	0,2687	1
w(Security guard)	0,0000	0,2000	0,0333	0,0745	3
w(Rapid response team)	0,0000	0,8000	0,3333	0,2981	2
w(Lawsuits handling)	0,0000	0,2000	0,0333	0,0745	3

Figure 6. Statistics of admissible weight-coefficients values for “external theft protection: organizational measures”

## EAS system

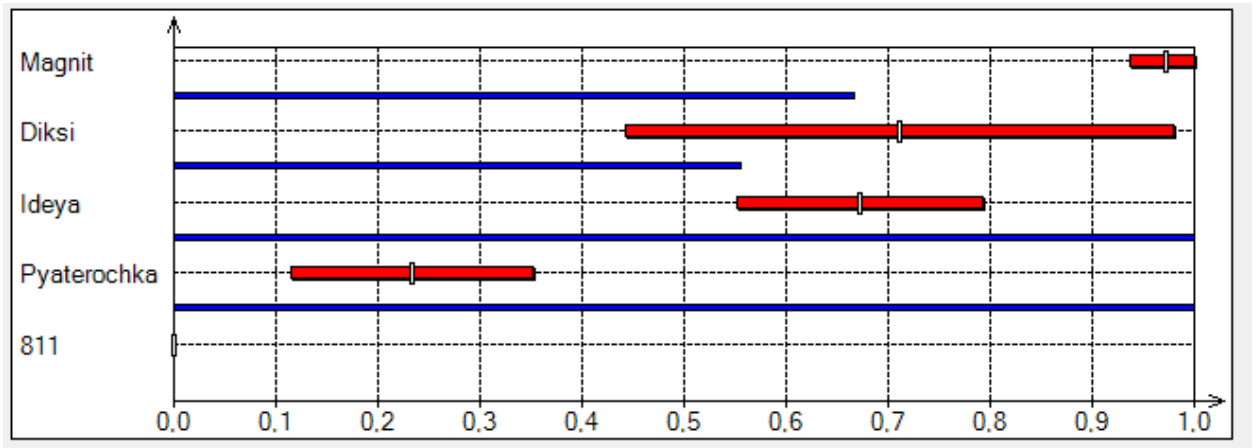


Figure 7. Aggregated preference indices visualization for EAS

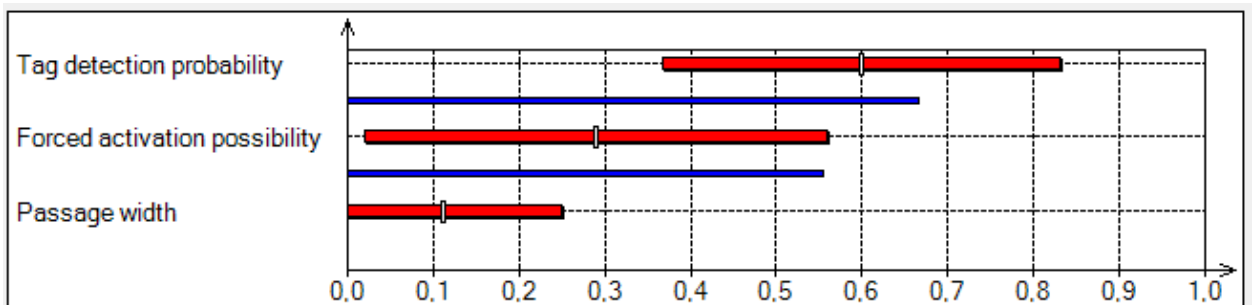


Figure 8. Weight-coefficients estimations visualization for EAS

Weight of index	Min	Max	Mean	StDev	Rank
w(Passage width)	0,0000	0,4000	0,1111	0,1370	3
w(Tag detection probability)	0,2000	1,0000	0,6000	0,2309	1
w(Forced activation possibility)	0,0000	0,8000	0,2889	0,2685	2

Figure 9. Statistics of admissible weight-coefficients values for EAS

## CCTV system

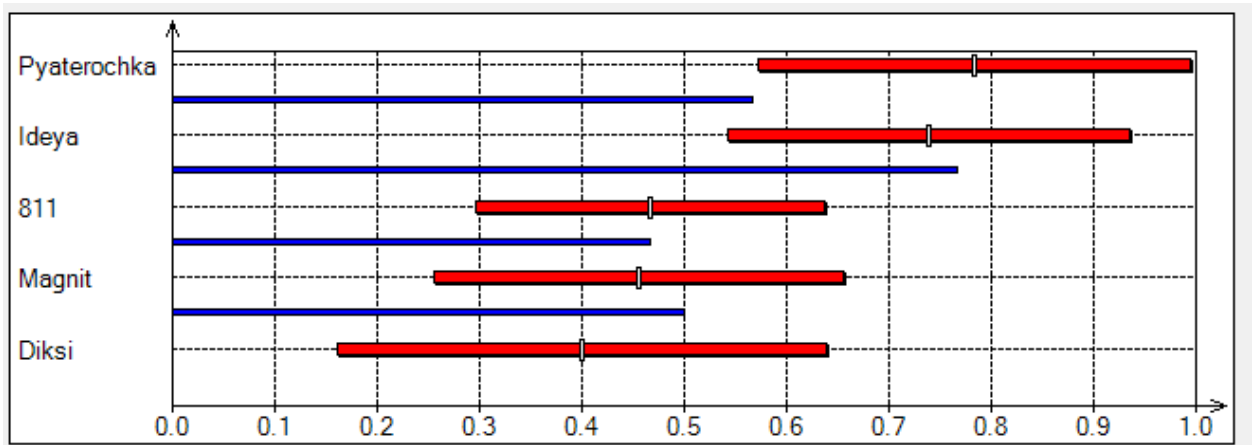


Figure 10. Aggregated preference indices visualization for CCTV

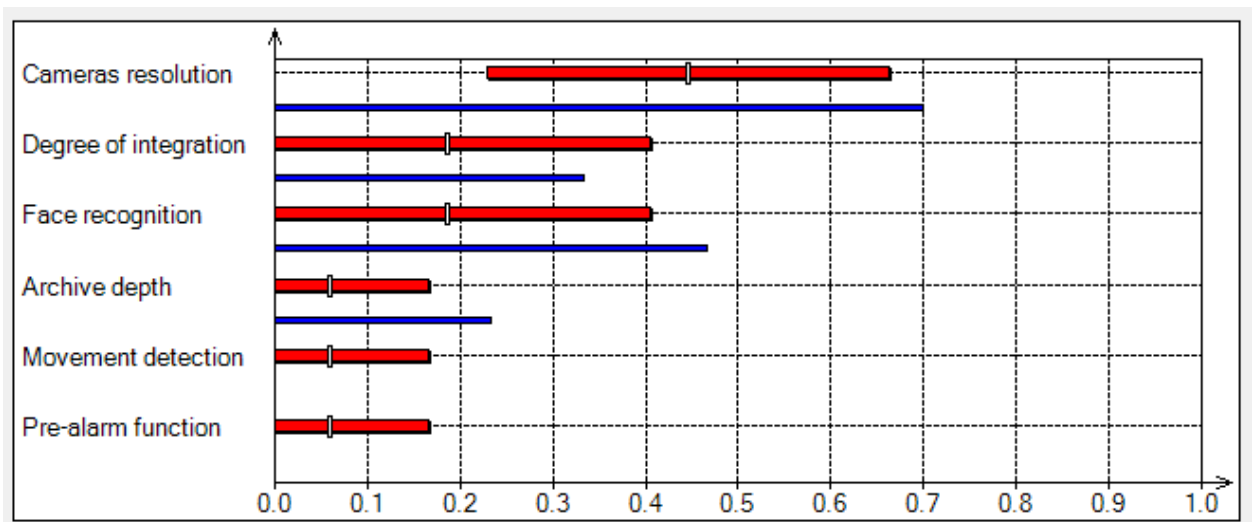


Figure 11. Weight-coefficients estimations visualization for CCTV

Weight of index	Min	Max	Mean	StDev	Rank
w(Cameras resolution)	0.2000	1.0000	0.4467	0.2172	1
w(Archive depth)	0.0000	0.4000	0.0600	0.1052	3
w(Movement detection)	0.0000	0.4000	0.0600	0.1052	3
w(Pre-alarm function)	0.0000	0.4000	0.0600	0.1052	3
w(Degree of integration)	0.0000	0.8000	0.1867	0.2187	2
w(Face recognition)	0.0000	0.8000	0.1867	0.2187	2

Figure 12. Statistics of admissible weight-coefficients values for CCTV



### External theft protection: technical measures

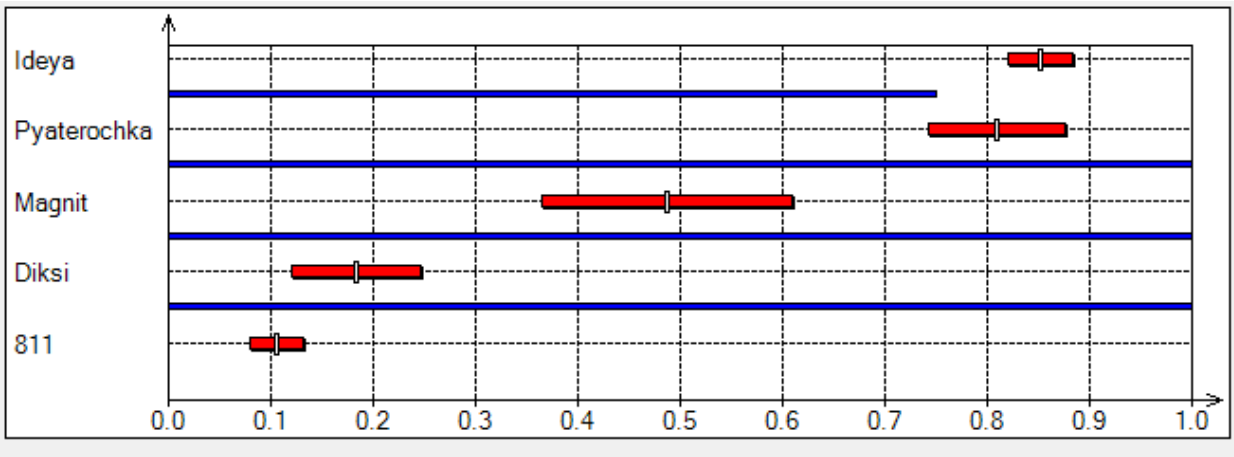


Figure 13. Aggregated preference indices visualization: external theft protection: technical measures

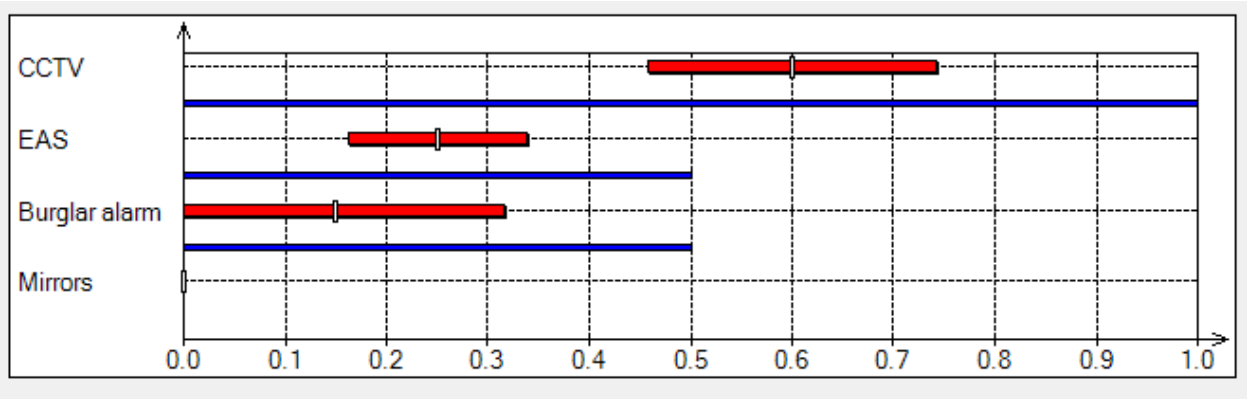


Figure 14. Weight-coefficients estimations visualization: external theft protection: technical measures

Weight of index	Min	Max	Mean	StDev	Rank
w(EAS)	0.2000	0.4000	0.2500	0.0866	2
w(CCTV)	0.4000	0.8000	0.6000	0.1414	1
w(Burglar alarm)	0.0000	0.4000	0.1500	0.1658	3
w(Mirrors)	0.0000	0.0000	0.0000	0.0000	4

Figure 15. Statistics of admissible weight-coefficients values for external theft protection: technical measures

## Supplier fraud protection: technical measures

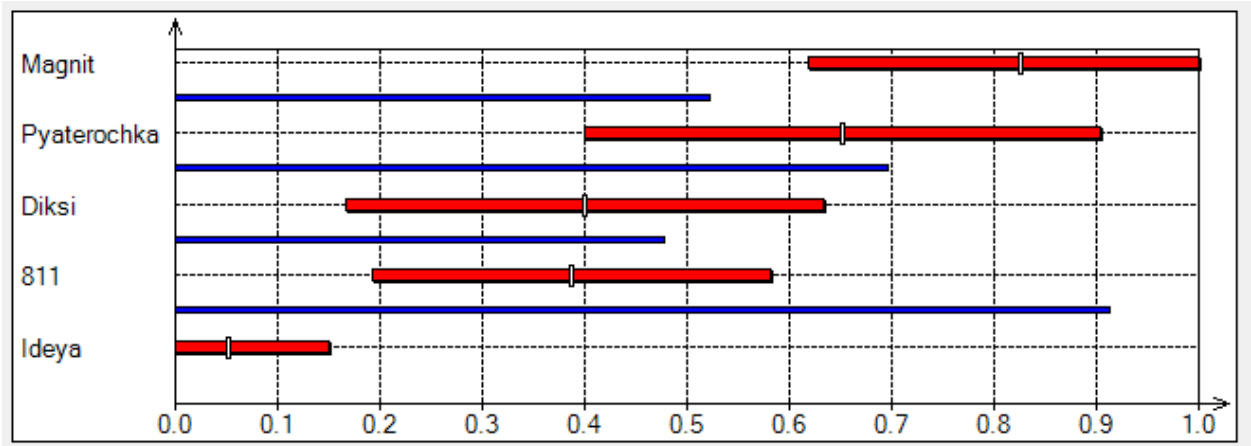


Figure 16. Aggregated preference indices visualization: supplier fraud protection: technical measures

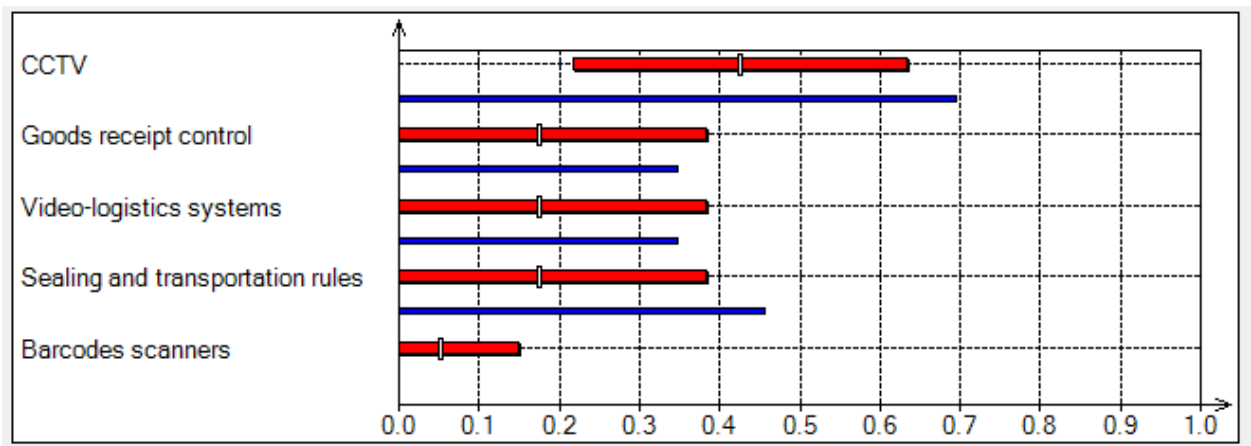


Figure 17. Weight-coefficients estimations visualization: supplier fraud protection: technical measures

Weight of index	Min	Max	Mean	StDev	Rank
w(CCTV)	0.2000	1.0000	0.4261	0.2069	1
w(Goods receipt control)	0.0000	0.8000	0.1739	0.2069	2
w(Barcodes scanners)	0.0000	0.4000	0.0522	0.0972	3
w(Video-logistics systems)	0.0000	0.8000	0.1739	0.2069	2
w(Sealing and transportation rules)	0.0000	0.8000	0.1739	0.2069	2

Figure 18. Statistics of admissible weight-coefficients values: supplier fraud protection: technical measures

Administrative error protection: organizational measures

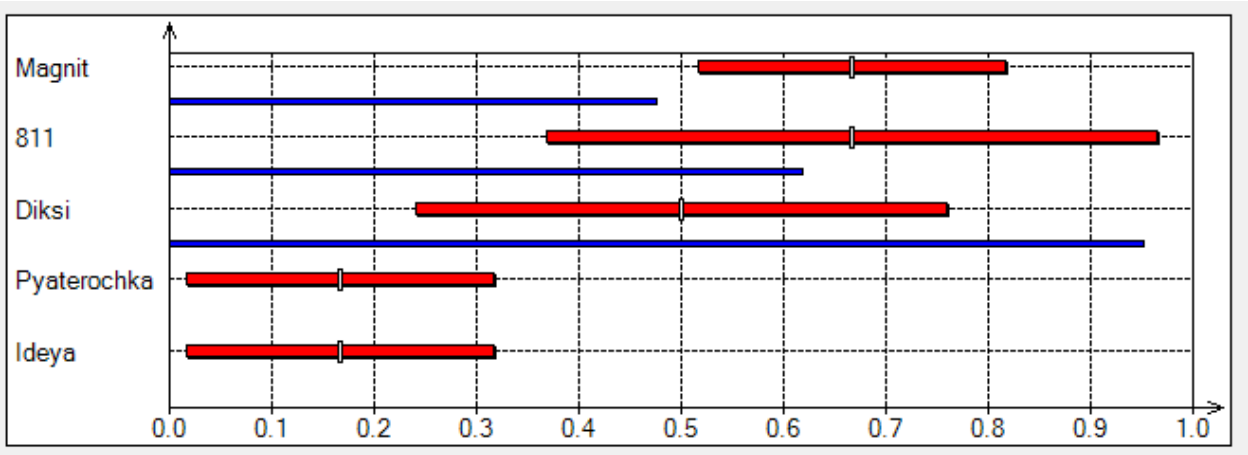


Figure 19. Aggregated preference indices visualization: administrative error protection: organizational measures

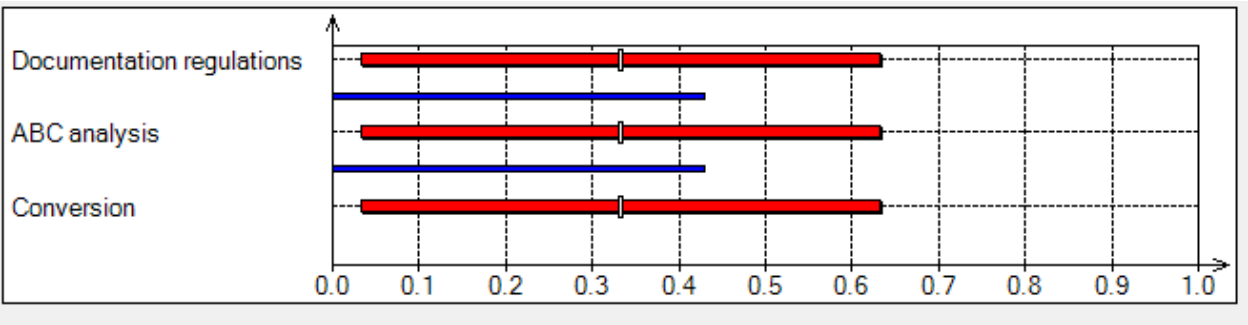


Figure 20. Weight-coefficients estimations visualization: administrative error protection: organizational measures

Weight of index	Min	Max	Mean	StDev	Rank
w(Documentation regulations)	0.0000	1.0000	0.3333	0.2981	1
w(ABC analysis)	0.0000	1.0000	0.3333	0.2981	1
w(Conversion)	0.0000	1.0000	0.3333	0.2981	1

Figure 21. Statistics of admissible weight-coefficients values: administrative error protection: organizational measures

## Administrative errors protection: technical measures

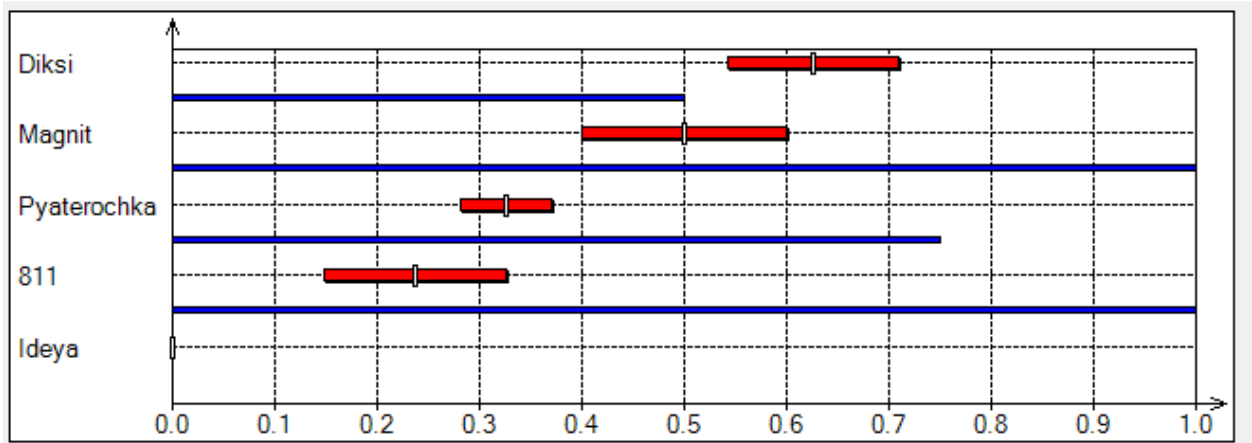


Figure 22. Aggregated preference indices visualization: administrative errors protection: technical measures

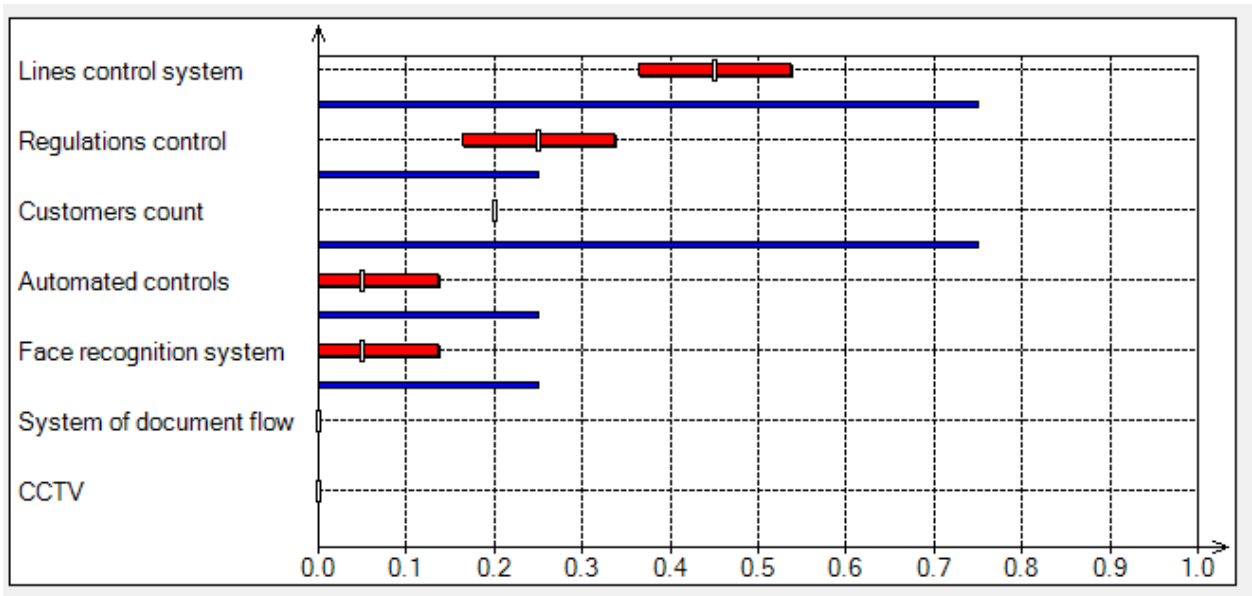


Figure 23. Weight-coefficients estimations visualization: administrative errors protection: technical measures

Weight of index	Min	Max	Mean	StDev	Rank
w(System of document flow)	0.0000	0.0000	0.0000	0.0000	5
w(Automated controls)	0.0000	0.2000	0.0500	0.0866	4
w(CCTV)	0.0000	0.0000	0.0000	0.0000	5
w(Lines control system)	0.4000	0.6000	0.4500	0.0866	1
w(Regulations control)	0.2000	0.4000	0.2500	0.0866	2
w(Customers count)	0.2000	0.2000	0.2000	0.0000	3
w(Face recognition system)	0.0000	0.2000	0.0500	0.0866	4

Figure 24. Statistics of admissible weight-coefficients values: administrative errors protection: technical measures

Cyber threat protection: organizational measures

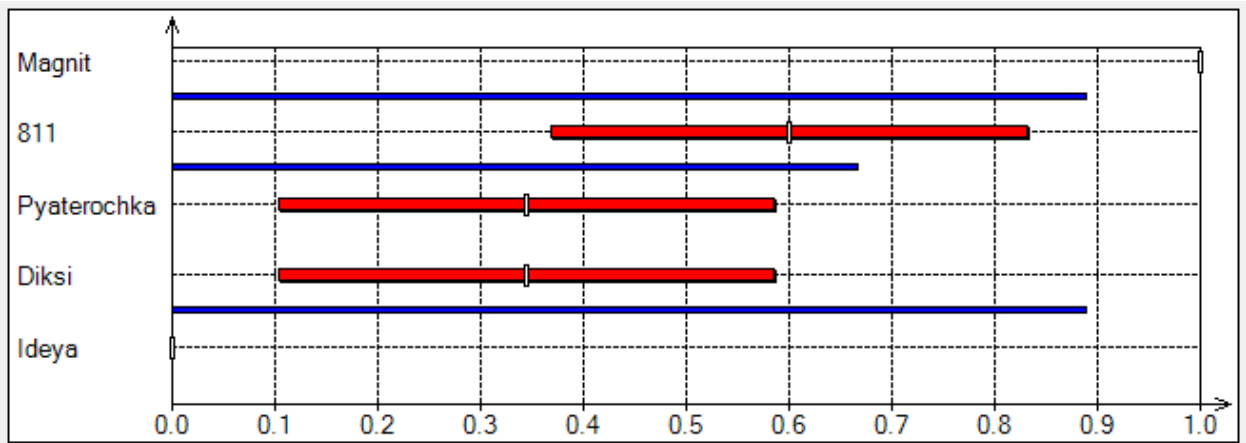


Figure 25. Aggregated preference indices visualization: cyber threat protection: organizational measures

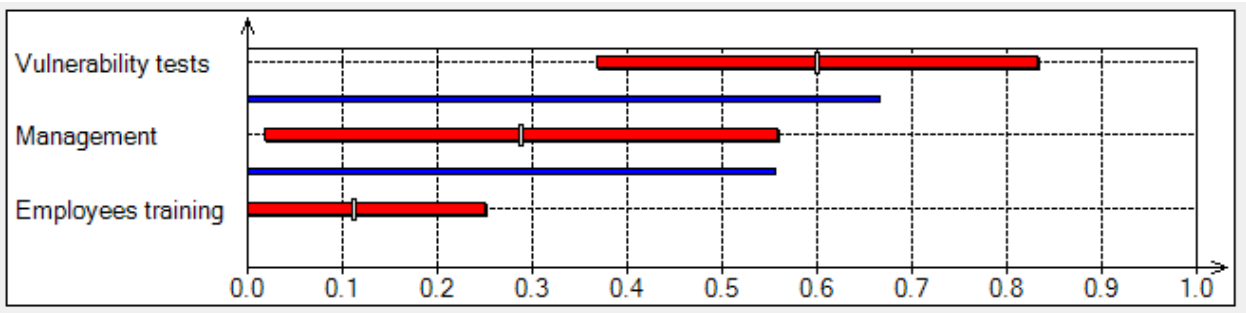


Figure 26. Weight-coefficients estimations visualization: cyber threat protection: organizational measures

Weight of index	Min	Max	Mean	StDev	Rank
w(Vulnerability tests)	0.2000	1.0000	0.6000	0.2309	1
w(Employees training)	0.0000	0.4000	0.1111	0.1370	3
w(Management)	0.0000	0.8000	0.2889	0.2685	2

Figure 27. Statistics of admissible weight-coefficients values: cyber threat protection: organizational measures

### Internal Theft Protection

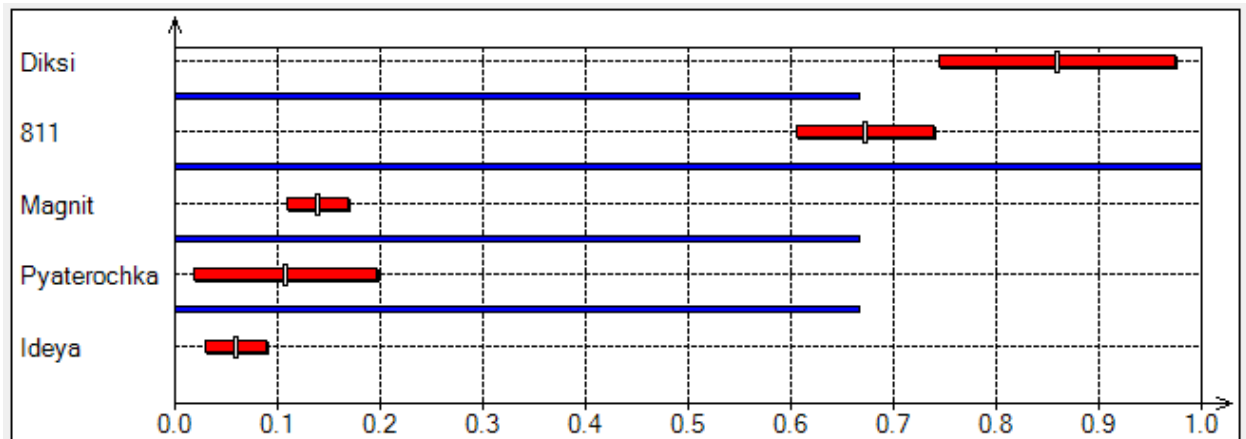


Figure 28. Aggregated preference indices visualization: Internal Theft Protection

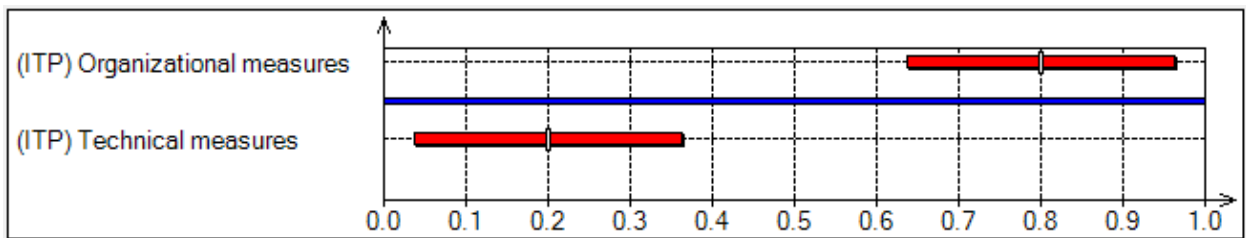


Figure 29. Weight-coefficients estimations visualization: Internal Theft Protection

Weight of index	Min	Max	Mean	StDev	Rank
w((ITP) Organizational measures)	0.6000	1.0000	0.8000	0.1633	1
w((ITP) Technical measures)	0.0000	0.4000	0.2000	0.1633	2

Figure 30. Statistics of admissible weight-coefficients values: Internal Theft Protection

### External Theft Protection

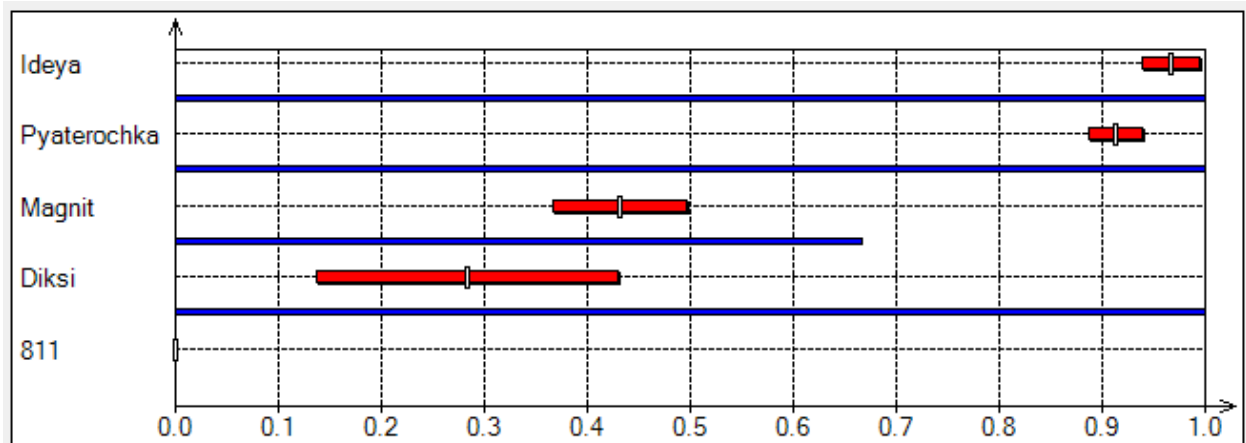


Figure 31. Aggregated preference indices visualization: External Theft Protection

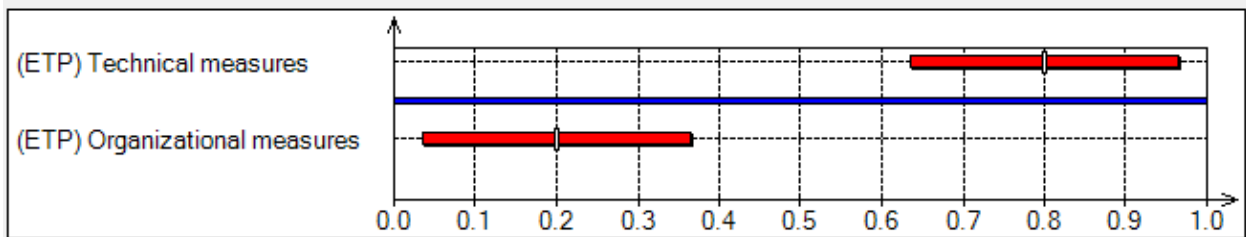


Figure 32. Weight-coefficients estimations visualization: External Theft Protection

Weight of index	Min	Max	Mean	StDev	Rank
w((ETP) Organizational measures)	0.0000	0.4000	0.2000	0.1633	2
w((ETP) Technical measures)	0.6000	1.0000	0.8000	0.1633	1

Figure 33. Statistics of admissible weight-coefficients values: External Theft Protection

Supplier Fraud Protection

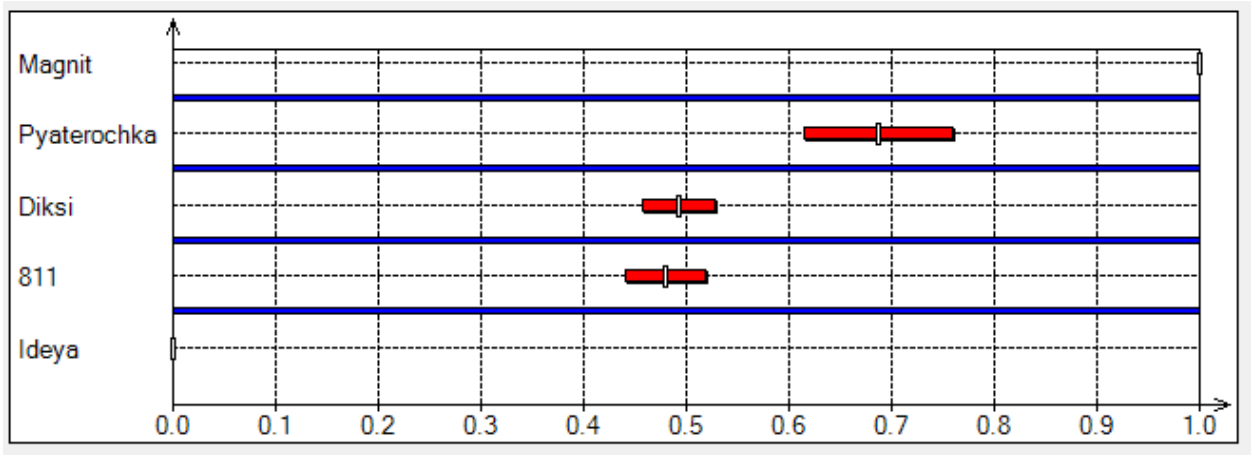


Figure 34. Aggregated preference indices visualization: Supplier Fraud Protection

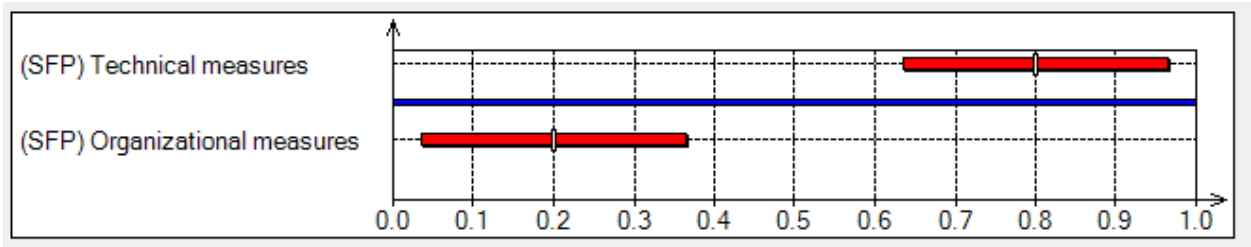


Figure 35. Weight-coefficients estimations visualization: Supplier Fraud Protection

Weight of index	Min	Max	Mean	StDev	Rank
w((SFP) Organizational measures)	0.0000	0.4000	0.2000	0.1633	2
w((SFP) Technical measures)	0.6000	1.0000	0.8000	0.1633	1

Figure 36. Statistics of admissible weight-coefficients values: Supplier Fraud Protection



### Administrative error protection

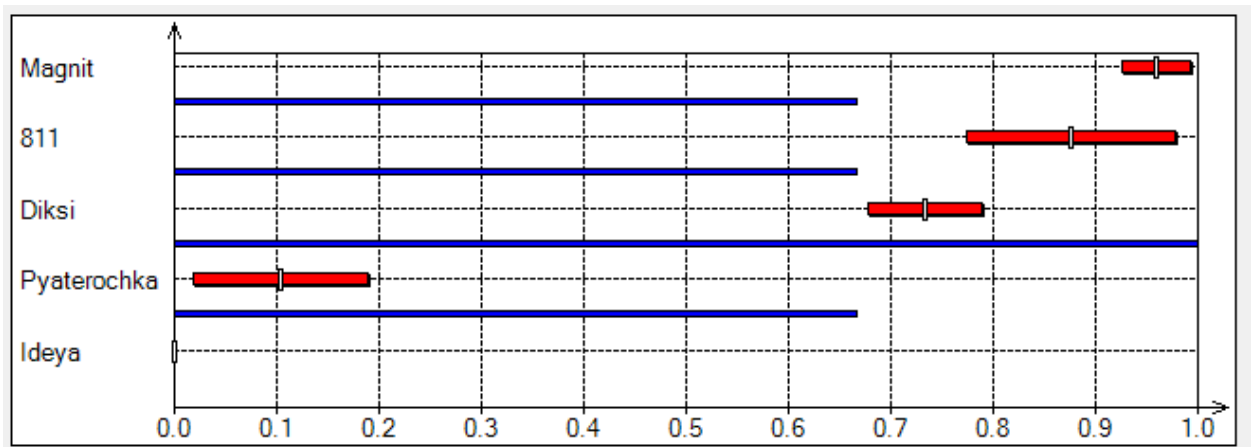


Figure 37. Aggregated preference indices visualization: administrative error protection

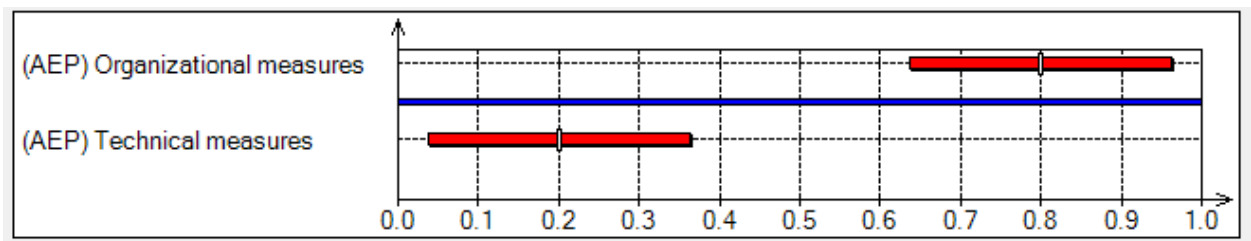


Figure 38. Weight-coefficients estimations visualization: administrative error protection

Weight of index	Min	Max	Mean	StDev	Rank
w((AEP) Organizational measures)	0.6000	1.0000	0.8000	0.1633	1
w((AEP) Technical measures)	0.0000	0.4000	0.2000	0.1633	2

Figure 39. Statistics of admissible weight-coefficients values: administrative error protection

Cyber threats protection

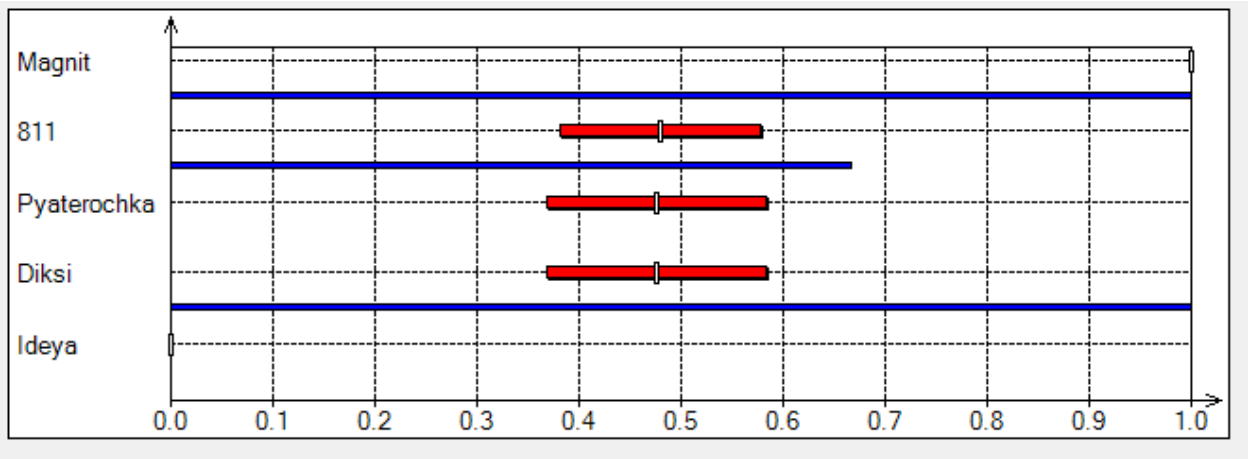


Figure 40. Aggregated preference indices visualization: cyber threats protection

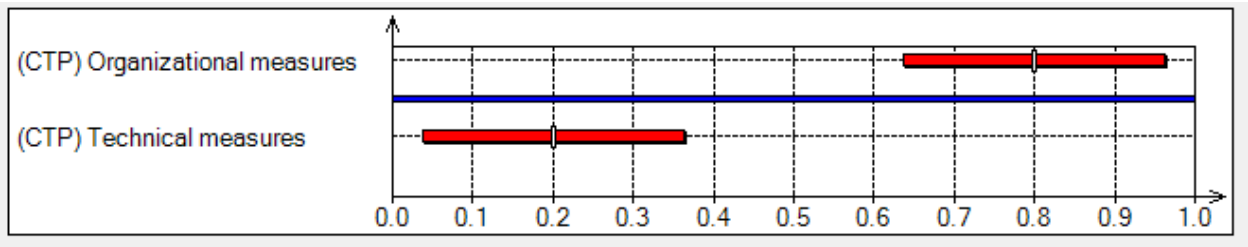


Figure 41. Weight-coefficients estimations visualization: cyber threats protection

Weight of index	Min	Max	Mean	StDev	Rank
w((CTP) Organizational measures)	0.6000	1.0000	0.8000	0.1633	1
w((CTP) Technical measures)	0.0000	0.4000	0.2000	0.1633	2

Figure 42. Statistics of admissible weight-coefficients values: cyber threats protection